

EXHIBIT 136

10/25/17 Google Terms of Service

GOOGLE TERMS OF SERVICE

Last modified: October 25, 2017 (view archived versions)

Welcome to Google!

Thanks for using our products and services ("Services"). The Services are provided by Google LLC ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

By using our Services, you are agreeing to these terms. Please read them carefully.

Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

Using our Services

You must follow any policies made available to you within the Services.

Don't misuse our Services. For example, don't interfere with our Services or try to access them using a method other than the interface and the instructions that we provide. You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations. We may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

Using our Services does not give you ownership of any intellectual property rights in our Services or the content you access. You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law. These terms do not grant you the right to use any branding or logos used in our Services. Don't remove, obscure, or alter any legal notices displayed in or along with our Services.

Our Services display some content that is not Google's. This content is the sole responsibility of the entity that makes it available. We may review content to determine whether it is illegal or violates our policies, and

we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do.

In connection with your use of the Services, we may send you service announcements, administrative messages, and other information. You may opt out of some of those communications.

Some of our Services are available on mobile devices. Do not use such Services in a way that distracts you and prevents you from obeying traffic or safety laws.

Your Google Account

You may need a Google Account in order to use some of our Services. You may create your own Google Account, or your Google Account may be assigned to you by an administrator, such as your employer or educational institution. If you are using a Google Account assigned to you by an administrator, different or additional terms may apply and your administrator may be able to access or disable your account.

To protect your Google Account, keep your password confidential. You are responsible for the activity that happens on or through your Google Account. Try not to reuse your Google Account password on third-party applications. If you learn of any unauthorized use of your password or Google Account, follow these instructions.

Privacy and Copyright Protection

Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.

We provide information to help copyright holders manage their intellectual property online. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center.

Your Content in our Services

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our Services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account. For example, you can choose your settings so your name and photo do not appear in an ad.

You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular Services. If you submit feedback or suggestions about our Services, we may use your feedback or suggestions without obligation to you.

About Software in our Services

When a Service requires or includes downloadable software, this software may update automatically on your device once a new version or feature is available. Some Services may let you adjust your automatic update

settings.

Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by these terms. You may not copy, modify, distribute, sell, or lease any part of our Services or included software, nor may you reverse engineer or attempt to extract the source code of that software, unless laws prohibit those restrictions or you have our written permission.

Open source software is important to us. Some software used in our Services may be offered under an open source license that we will make available to you. There may be provisions in the open source license that expressly override some of these terms.

Modifying and Terminating our Services

We are constantly changing and improving our Services. We may add or remove functionalities or features, and we may suspend or stop a Service altogether.

You can stop using our Services at any time, although we'll be sorry to see you go. Google may also stop providing Services to you, or add or create new limits to our Services at any time.

We believe that you own your data and preserving your access to such data is important. If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service.

Our Warranties and Disclaimers

We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we don't promise about our Services.

OTHER THAN AS EXPRESSLY SET OUT IN THESE TERMS OR ADDITIONAL TERMS, NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES "AS IS".

SOME JURISDICTIONS PROVIDE FOR CERTAIN WARRANTIES, LIKE THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE EXTENT PERMITTED BY LAW, WE EXCLUDE ALL WARRANTIES.

Liability for our Services

WHEN PERMITTED BY LAW, GOOGLE, AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES.

TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, FOR ANY CLAIMS UNDER THESE TERMS, INCLUDING FOR ANY IMPLIED WARRANTIES, IS LIMITED TO THE AMOUNT YOU PAID US TO USE THE SERVICES (OR, IF WE CHOOSE, TO SUPPLYING YOU THE SERVICES AGAIN).

IN ALL CASES, GOOGLE, AND ITS SUPPLIERS AND DISTRIBUTORS, WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE THAT IS NOT REASONABLY FORESEEABLE.

Business uses of our Services

If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits, judgments, litigation costs and attorneys' fees.

About these Terms

We may modify these terms or any additional terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should look at the terms regularly. We'll post notice of modifications to these terms on this page. We'll post notice of modified additional terms in the applicable Service. Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted. However, changes addressing new functions for a Service or changes made for legal

reasons will be effective immediately. If you do not agree to the modified terms for a Service, you should discontinue your use of that Service.

If there is a conflict between these terms and the additional terms, the additional terms will control for that conflict.

These terms control the relationship between Google and you. They do not create any third party beneficiary rights.

If you do not comply with these terms, and we don't take action right away, this doesn't mean that we are giving up any rights that we may have (such as taking action in the future).

If it turns out that a particular term is not enforceable, this will not affect any other terms.

The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

For information about how to contact Google, please visit our [contact page](#).

EXHIBIT 137

3/31/20 Google Terms of Service

GOOGLE TERMS OF SERVICE

Effective March 31, 2020

Archived versions

What's covered in these terms

We know it's tempting to skip these Terms of Service, but it's important to establish what you can expect from us as you use Google services, and what we expect from you.

These Terms of Service reflect the way Google's business works, the laws that apply to our company, and certain things we've always believed to be true. As a result, these Terms of Service help define Google's relationship with you as you interact with our services. For example, these terms include the following topic headings:

- What you can expect from us, which describes how we provide and develop our services
- What we expect from you, which establishes certain rules for using our services
- Content in Google services, which describes the intellectual property rights to the content you find in our services — whether that content belongs to you, Google, or others
- In case of problems or disagreements, which describes other legal rights you have, and what to expect in case someone violates these terms

Understanding these terms is important because, by using our services, you're agreeing to these terms.

Besides these terms, we also publish a Privacy Policy. Although it's not part of these terms, we encourage you to read it to better understand how you can update, manage, export, and delete your information.

Service provider

Google services are provided by, and you're contracting with:

Google LLC

organized under the laws of the State of Delaware, USA, and operating under the laws of the USA

1600 Amphitheatre Parkway
Mountain View, California 94043
USA

Age requirements

If you're under the age required to manage your own Google Account, you must have your parent or legal guardian's permission to use a Google Account. Please have your parent or legal guardian read these terms with you.

If you're a parent or legal guardian, and you allow your child to use the services, then these terms apply to you and you're responsible for your child's activity on the services.

Some Google services have additional age requirements as described in their service-specific additional terms and policies.

Your relationship with Google

These terms help define the relationship between you and Google. Broadly speaking, we give you permission to use our services if you agree to follow these terms, which reflect how Google's business works and how we earn money. When we speak of "Google," "we," "us," and "our," we mean Google LLC and its affiliates.

What you can expect from us

Provide a broad range of useful services

We provide a broad range of services that are subject to these terms, including:

- apps and sites (like Search and Maps)
- platforms (like Google Play)
- integrated services (like Maps embedded in other companies' apps or sites)
- devices (like Google Home)

Our services are designed to work together, making it easier for you to move from one activity to the next. For example, Maps can remind you to leave for an appointment that appears in your Google Calendar.

Improve Google services

We're constantly developing new technologies and features to improve our services. For example, we invest in artificial intelligence that uses machine learning to detect and block spam and malware, and to provide you with innovative features, like simultaneous translations. As part of this continual improvement, we sometimes add or remove features and functionalities, increase or decrease limits to our services, and start offering new services or stop offering old ones.

If we make material changes that negatively impact your use of our services or if we stop offering a service, we'll provide you with reasonable advance notice and an opportunity to export your content from your Google Account using Google Takeout, except in urgent situations such as preventing abuse, responding to legal requirements, or addressing security and operability issues.

What we expect from you

Follow these terms and service-specific additional terms

The permission we give you to use our services continues as long as you meet your responsibilities in:

- **these terms**
- **service-specific additional terms**, which could, for example, include things like additional age requirements

We also make various policies, help centers, and other resources available to you to answer common questions and to set expectations about using our services. These resources include our Privacy Policy, Copyright Help Center, Safety Center, and other pages accessible from our policies site.

Although we give you permission to use our services, we retain any intellectual property rights we have in the services.

Respect others

Many of our services allow you to interact with others. We want to maintain a respectful environment for everyone, which means you must follow these basic rules of conduct:

- comply with applicable laws, including export control, sanctions, and human trafficking laws
- respect the rights of others, including privacy and intellectual property rights
- don't abuse or harm others or yourself (or threaten or encourage such abuse or harm) — for example, by misleading, defrauding, defaming, bullying, harassing, or stalking others
- don't abuse, harm, interfere with, or disrupt the services

Our service-specific additional terms and policies provide additional details about appropriate conduct that everyone using those services must follow. If you find that others aren't following these rules, many of our services allow you to report abuse. If we act on a report of abuse, we also provide a fair process as described in the Taking action in case of problems section.

Permission to use your content

Some of our services are designed to let you upload, submit, store, send, receive, or share your content. You have no obligation to provide any content to our services and you're free to choose the content that you want to provide. If you choose to upload or share content, please make sure you have the necessary rights to do so and that the content is lawful.

License

Your content remains yours, which means that you retain any intellectual property rights that you have in your content. For example, you have intellectual property rights in the creative content you make, such as reviews you write. Or you may have the right to share someone else's creative content if they've given you their permission.

We need your permission if your intellectual property rights restrict our use of your content. You provide Google with that permission through this license.

What's covered

This license covers your content if that content is protected by intellectual property rights.

What's not covered

- This license doesn't affect your privacy rights — it's only about your intellectual property rights
- This license doesn't cover these types of content:
 - publicly-available factual information that you provide, such as corrections to the address of a local business. That information doesn't require a license because it's considered common knowledge that everyone's free to use.
 - feedback that you offer, such as suggestions to improve our services. Feedback is covered in the Service-related communications section below.

Scope

This license is:

- worldwide, which means it's valid anywhere in the world
- non-exclusive, which means you can license your content to others
- royalty-free, which means there are no fees for this license

Rights

This license allows Google to:

- host, reproduce, distribute, communicate, and use your content — for example, to save your content on our systems and make it accessible from anywhere you go
- publish, publicly perform, or publicly display your content, if you've made it visible to others
- modify and create derivative works based on your content, such as reformatting or translating it
- sublicense these rights to:
 - other users to allow the services to work as designed, such as enabling you to share photos with people you choose
 - our contractors who've signed agreements with us that are consistent with these terms, only for the limited purposes described in the Purpose section below

Purpose

This license is for the limited purpose of:

- **operating and improving the services**, which means allowing the services to work as designed and creating new features and functionalities. This includes using automated systems and algorithms to analyze your content:
 - for spam, malware, and illegal content

- to recognize patterns in data, such as determining when to suggest a new album in Google Photos to keep related photos together
- to customize our services for you, such as providing recommendations and personalized search results, content, and ads (which you can change or turn off in Ads Settings)

This analysis occurs as the content is sent, received, and when it is stored.

- **using content you've shared publicly to promote the services.** For example, to promote a Google app, we might quote a review you wrote. Or to promote Google Play, we might show a screenshot of the app you offer in the Play Store.
- **developing new technologies and services** for Google consistent with these terms

Duration

This license lasts for as long as your content is protected by intellectual property rights.

If you remove from our services any content that's covered by this license, then our systems will stop making that content publicly available in a reasonable amount of time. There are two exceptions:

- If you already shared your content with others before removing it. For example, if you shared a photo with a friend who then made a copy of it, or shared it again, then that photo may continue to appear in your friend's Google Account even after you remove it from your Google Account.
- If you make your content available through other companies' services, it's possible that search engines, including Google Search, will continue to find and display your content as part of their search results.

Using Google services

Your Google Account

If you meet these age requirements you can create a Google Account for your convenience. Some services require that you have a Google Account in order to work — for example, to use Gmail, you need a Google Account so that you have a place to send and receive your email.

You're responsible for what you do with your Google Account, including taking reasonable steps to keep your Google Account secure, and we encourage you to regularly use the Security Checkup.

Using Google services on behalf of an organization

Many organizations, such as businesses, non-profits, and schools, take advantage of our services. To use our services on behalf of an organization:

- an authorized representative of that organization must agree to these terms
- your organization's administrator may assign a Google Account to you. That administrator might require you to follow additional rules and may be able to access or disable your Google Account.

Service-related communications

To provide you with our services, we sometimes send you service announcements and other information. To learn more about how we communicate with you, see Google's Privacy Policy.

If you choose to give us feedback, such as suggestions to improve our services, we may act on your feedback without obligation to you.

Content in Google services

Your content

Some of our services give you the opportunity to make your content publicly available — for example, you might post a product or restaurant review that you wrote, or you might upload a blog post that you created.

- See the [Permission to use your content](#) section for more about your rights in your content, and how your content is used in our services
- See the [Removing your content](#) section to learn why and how we might remove user-generated content from our services

If you think someone is infringing your intellectual property rights, you can send us notice of the infringement and we'll take appropriate action. For example, we suspend or close the Google Accounts of repeat copyright infringers as described in our [Copyright Help Center](#).

Google content

Some of our services include content that belongs to Google — for example, many of the visual illustrations you see in Google Maps. You may use Google's content as allowed by these terms and any service-specific additional terms, but we retain any intellectual property rights that we have in our content. Don't remove, obscure, or alter any of our branding, logos, or legal notices. If you want to use our branding or logos, please see the [Google Brand Permissions](#) page.

Other content

Finally, some of our services give you access to content that belongs to other people or organizations — for example, a store owner's description of their own business, or a newspaper article displayed in Google News. You may not use this content without that person or organization's permission, or as otherwise allowed by law. The views expressed in other people or organizations' content are theirs, and don't necessarily reflect Google's views.

Software in Google services

Some of our services include downloadable software. We give you permission to use that software as part of the services.

The license we give you is:

- worldwide, which means it's valid anywhere in the world
- non-exclusive, which means that we can license the software to others
- royalty-free, which means there are no fees for this license
- personal, which means it doesn't extend to anyone else
- non-assignable, which means you're not allowed to assign the license to anyone else

Some of our services include software that's offered under open source license terms that we make available to you. Sometimes there are provisions in the open source license that explicitly override parts of these terms, so please be sure to read those licenses.

You may not copy, modify, distribute, sell, or lease any part of our services or software. Also, you may not reverse engineer or attempt to extract any of our source code unless you have our written permission or applicable law lets you do so.

When a service requires or includes downloadable software, that software sometimes updates automatically on your device once a new version or feature is available. Some services let you adjust your automatic update settings.

In case of problems or disagreements

By law, you have the right to (1) a certain quality of service, and (2) ways to fix problems if things go wrong. These terms don't limit or take away any of those rights. For example, if you're a consumer, then you continue to enjoy all legal rights granted to consumers under applicable law.

Warranty

We provide our services using reasonable skill and care. If we don't meet the quality level described in this warranty, you agree to tell us and we'll work with you to try to resolve the issue.

Disclaimers

The only commitments we make about our services (including the content in the services, the specific functions of our services, or their reliability, availability, or ability to meet your needs) are (1) described in the Warranty section, (2) stated in the service-specific additional terms, or (3) provided under applicable laws. We don't make any other commitments about our services.

And unless required by law, we don't provide implied warranties, such as the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Liabilities

For all users

These terms only limit our responsibilities as allowed by applicable law. Specifically, these terms don't limit Google's liability for death or personal injury, fraud, fraudulent misrepresentation, gross negligence, or willful misconduct.

Other than the rights and responsibilities described in this section (In case of problems or disagreements), Google won't be responsible for any other losses, unless they're caused by our breach of these terms or service-specific additional terms.

For business users and organizations only

If you're a business user or organization, then to the extent allowed by applicable law:

- You'll indemnify Google and its directors, officers, employees, and contractors for any third-party legal proceedings (including actions by government authorities) arising out of or relating to your unlawful use of the services or violation of these terms or service-specific additional terms. This indemnity covers any liability or expense arising from claims, losses, damages, judgments, fines, litigation costs, and legal fees.
- Google won't be responsible for the following liabilities:
 - loss of profits, revenues, business opportunities, goodwill, or anticipated savings
 - indirect or consequential loss
 - punitive damages
- Google's total liability arising out of or relating to these terms is limited to the greater of (1) US\$500 or (2) 125% of the fees that you paid to use the relevant services in the 12 months before the breach

If you're legally exempt from certain responsibilities, including indemnification, then those responsibilities don't apply to you under these terms. For example, the United Nations enjoys certain immunities from legal obligations and these terms don't override those immunities.

Taking action in case of problems

Before taking action as described below, we'll provide you with advance notice when reasonably possible, describe the reason for our action, and give you an opportunity to fix the problem, unless we reasonably believe that doing so would:

- cause harm or liability to a user, third party, or Google
- violate the law or a legal enforcement authority's order
- compromise an investigation
- compromise the operation, integrity, or security of our services

Removing your content

If we reasonably believe that any of your content (1) breaches these terms, service-specific additional terms or policies, (2) violates applicable law, or (3) could harm our users, third parties, or Google, then we reserve the right to take down some or all of that content in accordance with applicable law. Examples include child pornography, content that facilitates human trafficking or harassment, and content that infringes someone else's intellectual property rights.

Suspending or terminating your access to Google services

Google reserves the right to suspend or terminate your access to the services or delete your Google Account if any of these things happen:

- you materially or repeatedly breach these terms, service-specific additional terms or policies
- we're required to do so to comply with a legal requirement or a court order
- we reasonably believe that your conduct causes harm or liability to a user, third party, or Google — for example, by hacking, phishing, harassing, spamming, misleading others, or scraping content that doesn't belong to you

If you believe your Google Account has been suspended or terminated in error, you can appeal.

Of course, you're always free to stop using our services at any time. If you do stop using a service, we'd appreciate knowing why so that we can continue improving our services.

Settling disputes, governing law, and courts

For information about how to contact Google, please visit our contact page.

California law will govern all disputes arising out of or relating to these terms, service-specific additional terms, or any related services, regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

To the extent that applicable local law prevents certain disputes from being resolved in a California court, then you can file those disputes in your local courts. Likewise, if applicable local law prevents your local

court from applying California law to resolve these disputes, then these disputes will be governed by the applicable local laws of your country, state, or other place of residence.

About these terms

By law, you have certain rights that can't be limited by a contract like these terms of service. These terms are in no way intended to restrict those rights.

These terms describe the relationship between you and Google. They don't create any legal rights for other people or organizations, even if others benefit from that relationship under these terms.

We want to make these terms easy to understand, so we've used examples from our services. But not all services mentioned may be available in your country.

If these terms conflict with the service-specific additional terms, the additional terms will govern for that service.

If it turns out that a particular term is not valid or enforceable, this will not affect any other terms.

If you don't follow these terms or the service-specific additional terms, and we don't take action right away, that doesn't mean we're giving up any rights that we may have, such as taking action in the future.

We may update these terms and service-specific additional terms (1) to reflect changes in our services or how we do business — for example, when we add new services, features, technologies, pricing, or benefits (or remove old ones), (2) for legal, regulatory, or security reasons, or (3) to prevent abuse or harm.

If we materially change these terms or service-specific additional terms, we'll provide you with reasonable advance notice and the opportunity to review the changes, except (1) when we launch a new service or feature, or (2) in urgent situations, such as preventing ongoing abuse or responding to legal requirements. If you don't agree to the new terms, you should remove your content and stop using the services. You can also end your relationship with us at any time by closing your Google Account.

DEFINITIONS

affiliate

An entity that belongs to the Google group of companies, which means Google LLC and its subsidiaries, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, and Google Dialer Inc.

business user

An individual or entity who is not a consumer (see consumer).

consumer

An individual who uses Google services for personal, non-commercial purposes outside of their trade, business, craft, or profession. (See business user)

copyright

A legal right that allows the creator of an original work (such as a blog post, photo, or video) to decide if and how that original work may be used by others.

disclaimer

A statement that limits someone's legal responsibilities.

EU Platform-to-Business Regulation

The Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services.

indemnify or indemnity

An individual or organization's contractual obligation to compensate the losses suffered by another individual or organization from legal proceedings such as lawsuits.

intellectual property rights (IP rights)

Rights over the creations of a person's mind, such as inventions (patent rights); literary and artistic works (copyright); designs (design rights); and symbols, names, and images used in commerce (trademarks). IP rights may belong to you, another individual, or an organization.

liability

Losses from any type of legal claim, whether the claim is based on a contract, tort (including negligence), or other reason, and whether or not those losses could have been reasonably anticipated or foreseen.

organization

A legal entity (such as a corporation, non-profit, or school) and not an individual person.

services

Google services that are subject to these terms are the products and services listed at <https://policies.google.com/terms/service-specific>, including:

- Google apps and sites (like Search and Maps)
- platforms (like Google Play)
- integrated services (like Maps embedded in other companies' apps or sites)
- devices (like Google Home)

trademark

Symbols, names, and images used in commerce that are capable of distinguishing the goods or services of one individual or organization from those of another.

warranty

An assurance that a product or service will perform to a certain standard.

your content

Things that you write, upload, submit, store, send, receive, or share with Google using our services, such as:

- Docs, Sheets, and Slides you create
- blog posts you upload through Blogger
- reviews you submit through Maps
- videos you store in Drive
- emails you send and receive through Gmail
- pictures you share with friends through Photos
- travel itineraries that you share with Google

EXHIBIT 138

1/5/22 Google Terms of Service

GOOGLE TERMS OF SERVICE

Effective 5 January 2022

[Archived versions](#)

What's covered in these terms

We know it's tempting to skip these Terms of Service, but it's important to establish what you can expect from us as you use Google services, and what we expect from you.

These Terms of Service reflect [the way that Google's business works](#), the laws that apply to our company, and [certain things that we've always believed to be true](#). As a result, these Terms of Service help define Google's relationship with you as you interact with our services. For example, these terms include the following topic headings:

- [What you can expect from us](#), which describes how we provide and develop our services
- [What we expect from you](#), which establishes certain rules for using our services
- [Content in Google services](#), which describes the intellectual property rights to the content that you find in our services – whether that content belongs to you, Google or others
- [In case of problems or disagreements](#), which describes other legal rights that you have, and what to expect in case someone violates these terms.

Understanding these terms is important because, by using our services, you're agreeing to these terms.

In addition to these terms, we also publish a [Privacy Policy](#). We encourage you to read it to better understand how you can [update, manage, export and delete your information](#).

Terms

Service provider

Google [services](#) are provided by, and you're contracting with:

Google LLC

organised under the laws of the State of Delaware, USA, and operating under the laws of the USA

1600 Amphitheatre Parkway
Mountain View, California 94043
USA

Age requirements

If you're under the [age required to manage your own Google Account](#), you must have your parent or legal guardian's permission to use a Google Account. Please ask your parent or legal guardian to read these terms with you.

If you're a parent or legal guardian, and you allow your child to use the [services](#), then these terms apply to you and you're responsible for your child's activity on the services.

Some Google services have additional age requirements as described in their [service-specific additional terms and policies](#).

Your relationship with Google

These terms help define the relationship between you and Google. Broadly speaking, we give you permission to use our [services](#) if you agree to follow these terms, which reflect [how Google's business works and how we earn money](#). When we speak of 'Google', 'we', 'us' and 'our', we mean Google LLC and its [affiliates](#).

What you can expect from us

Provide a broad range of useful services

We provide a broad range of services that are subject to these terms, including:

- apps and sites (like Search and Maps)
- platforms (like Google Shopping)
- integrated services (like Maps embedded in other companies' apps or sites)
- devices (like Google Nest)

Many of these services also include content that you can stream or interact with.

Our services are designed to work together, making it easier for you to move from one activity to the next. For example, if your Calendar event includes an address, you can click on that address and Maps can show you how to get there.

Develop, improve and update Google services

We're constantly developing new technologies and features to improve our services. For example, we use artificial intelligence and machine learning to provide you with simultaneous translations and to better detect and block spam and malware. As part of this continual improvement, we sometimes add or remove features and functionalities, increase or decrease limits to our services and start offering new services or stop offering old ones. When a service requires or includes downloadable software, that software sometimes updates automatically on your device once a new version or feature is available. Some services let you adjust your automatic update settings.

If we make material changes that negatively impact your use of our services or if we stop offering a service, we'll provide you with reasonable advance notice, except in urgent situations such as preventing abuse, responding to legal requirements or addressing security and operability issues. We'll also provide you with an opportunity to export your content from your Google Account using [Google Takeout](#), subject to applicable law and policies.

What we expect from you

Follow these terms and service-specific additional terms

The permission that we give you to use our services continues as long as you comply with:

- **these terms**

- [service-specific additional terms](#), which could, for example, include things like additional age requirements

You also agree that our [Privacy Policy](#) applies to your use of our services. Additionally, we provide resources such as the [Copyright Help Centre](#) and [Safety Centre](#), as well as descriptions of our technologies from our [policies site](#) to answer common questions and to set expectations about using our services.

Although we give you permission to use our services, we retain any [intellectual property rights](#) that we have in the services.

Respect others

We want to maintain a respectful environment for everyone, which means that you must follow these basic rules of conduct:

- comply with applicable laws, including export control, sanctions and human trafficking laws
- respect the rights of others, including privacy and intellectual property rights
- don't abuse or harm others or yourself (or threaten or encourage such abuse or harm) – for example, by misleading, defrauding, illegally impersonating, defaming, bullying, harassing or stalking others
- don't abuse, harm, interfere with or disrupt the services – for example, by accessing or using them in fraudulent or deceptive ways, introducing malware or spamming, hacking or bypassing our systems or protective measures. When we index the web to bring you search results, we respect standard usage restrictions that website owners specify in their websites' code, so we require the same when others use our services

Our [service-specific additional terms and policies](#) provide additional details about appropriate conduct that everyone using those services must follow. If you find that others aren't following these rules, many of our services allow you to [report abuse](#). If we act on a report of abuse, we also provide the process described in the [Taking action in case of problems](#) section.

Permission to use your content

Some of our services are designed to let you upload, submit, store, send, receive or share [your content](#). You have no obligation to provide any content to our services and you're free to choose the content that you want

to provide. If you choose to upload or share content, please make sure that you have the necessary rights to do so and that the content is lawful.

Licence

Your content remains yours, which means that you retain any intellectual property rights that you have in your content. For example, you have intellectual property rights in the creative content that you make, such as reviews that you write. Or you may have the right to share someone else's creative content if they've given you their permission.

We need your permission if your intellectual property rights restrict our use of your content. You provide Google with that permission through this licence.

What's covered

This licence covers your content if that content is protected by intellectual property rights.

What's not covered

- This licence doesn't affect your privacy rights – it's only about your intellectual property rights
- This licence doesn't cover these types of content:
 - publicly available, factual information that you provide, such as corrections to the address of a local business. That information doesn't require a licence because it's considered common knowledge that everyone's free to use.
 - feedback that you offer, such as suggestions to improve our services. Feedback is covered in the [Service-related communications](#) section below.

Scope

This licence is:

- worldwide, which means that it's valid anywhere in the world
- non-exclusive, which means that you can licence your content to others

- royalty-free, which means that there are no monetary fees for this licence

Rights

This licence allows Google to:

- host, reproduce, distribute, communicate and use your content – for example, to save your content on our systems and make it accessible from anywhere that you go
- publish, publicly perform or publicly display your content, if you've made it visible to others
- modify and create derivative works based on your content, such as reformatting or translating it
- sublicense these rights to:
 - other users to allow the services to work as designed, such as enabling you to share photos with people that you choose
 - our contractors who've signed agreements with us that are consistent with these terms, only for the limited purposes described in the [Purpose](#) section below

Purpose

This licence is for the limited purpose of:

- **operating and improving the services**, which means allowing the services to work as designed and creating new features and functionalities. This includes using automated systems and algorithms to analyse your content:
 - for spam, malware and illegal content
 - to recognise patterns in data, such as determining when to suggest a new album in Google Photos to keep related photos together
 - to customise our services for you, such as providing recommendations and personalised search results, content and ads (which you can change or turn off in [Ad Settings](#))

This analysis occurs as the content is sent, received and when it is stored.

- **using content that you've shared publicly to promote the services.** For example, to promote a Google app, we might quote a review that you wrote. Or to promote Google Play, we might show a screenshot of the app that you offer in the Play Store.
- **developing new technologies and services** for Google consistent with these terms

Duration

This licence lasts for as long as your content is protected by intellectual property rights.

If you remove from our services any content that's covered by this licence, our systems will stop making that content publicly available in a reasonable amount of time. There are two exceptions:

- If you already shared your content with others before removing it. For example, if you shared a photo with a friend who then made a copy of it, or shared it again, then that photo may continue to appear in your friend's Google Account even after you remove it from your Google Account.
- If you make your content available through other companies' services, it's possible that search engines, including Google Search, will continue to find and display your content as part of their search results.

Using Google services

Your Google Account

If you meet [these age requirements](#), you can [create a Google Account](#) for your convenience. Some [services](#) require that you have a Google Account in order to work – for example, to use Gmail, you need a Google Account so that you have a place to send and receive your email.

You're responsible for what you do with your Google Account, including taking reasonable steps to keep your Google Account secure, and we encourage you to regularly use the [Security Check-Up](#).

Using Google services on behalf of an organisation or business

Many [organisations](#), such as businesses, non-profits and schools, take advantage of our [services](#). To use our services on behalf of an organisation:

- an authorised representative of that organisation must agree to these terms
- your organisation's administrator may assign a Google Account to you. That administrator might require you to follow additional rules and may be able to access or disable your Google Account.

Service-related communications

To provide you with our services, we sometimes send you service announcements and other information. To learn more about how we communicate with you, see Google's [Privacy Policy](#).

If you choose to give us feedback, such as suggestions to improve our services, we may act on your feedback without obligation to you.

Content in Google services

Your content

Some of our [services](#) give you the opportunity to make your content publicly available – for example, you might post a product or restaurant review that you wrote, or you might upload a blog post that you created.

- See the [Permission to use your content](#) section for more about your rights in [your content](#), and how your content is used in our services
- See the [Removing your content](#) section to learn why and how we might remove user-generated content from our services

If you think that someone is infringing your [intellectual property rights](#), you can [send us notice of the infringement](#) and we'll take appropriate action. For example, we suspend or close the Google Accounts of

repeat [copyright infringers](#) as described in our [Copyright Help Centre](#).

Google content

Some of our [services](#) include content that belongs to Google – for example, many of the visual illustrations that you see in Google Maps. You may use Google’s content as allowed by these terms and any [service-specific additional terms](#), but we retain any intellectual property rights that we have in our content. Don’t remove, obscure or alter any of our branding, logos or legal notices. If you want to use our branding or logos, please see the [Google Brand Permissions](#) page.

Other content

Finally, some of our [services](#) give you access to content that belongs to other people or [organisations](#) – for example, a store owner’s description of their own business, or a newspaper article displayed in Google News. You may not use this content without that person or organisation’s permission, or as otherwise allowed by law. The views expressed in the content of other people or organisations are their own, and don’t necessarily reflect Google’s views.

Software in Google services

Some of our [services](#) include downloadable software. We give you permission to use that software as part of the services.

The licence that we give you is:

- worldwide, which means that it’s valid anywhere in the world
- non-exclusive, which means that we can licence the software to others
- royalty-free, which means that there are no monetary fees for this licence
- personal, which means that it doesn’t extend to anyone else
- non-assignable, which means that you’re not allowed to assign the licence to anyone else

Some of our services include software that's offered under open-source licence terms that we make available to you. Sometimes there are provisions in the open-source licence that explicitly override parts of these terms, so please make sure that you read those licences.

You may not copy, modify, distribute, sell or lease any part of our services or software.

In case of problems or disagreements

Warranty disclaimer

We built our reputation on providing useful, reliable services like Google Search and Maps, and we're continuously improving our services to meet your needs. However, for legal purposes, we offer our [services](#) without [warranties](#) unless explicitly stated in our [service-specific additional terms](#). The law requires that we explain this using specific legal language and that we use capital letters to help make sure that you see it, as follows:

TO THE EXTENT ALLOWED BY APPLICABLE LAW, WE PROVIDE OUR SERVICES 'AS IS' WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. FOR EXAMPLE, WE DON'T MAKE ANY WARRANTIES ABOUT THE CONTENT OR FEATURES OF THE SERVICES, INCLUDING THEIR ACCURACY, RELIABILITY, AVAILABILITY OR ABILITY TO MEET YOUR NEEDS.

Liabilities

For all users

Both the law and these terms try to strike a balance as to what you or Google can claim from the other in case of problems. That's why the law allows us to limit certain [liabilities](#) – but not others – under these terms.

These terms only limit our responsibilities as allowed by applicable law. These terms don't limit liability for gross negligence or willful misconduct.

To the extent allowed by applicable law:

- Google is liable only for its breaches of these terms or applicable [service-specific additional terms](#)
- Google isn't liable for:
 - loss of profits, revenues, business opportunities, goodwill or anticipated savings
 - indirect or consequential losses
 - punitive damages
- Google's total liability arising out of or relating to these terms is limited to the greater of (1) \$200 or (2) the fees paid to use the relevant services in the 12 months before the dispute

For business users and organisations only

If you're a [business user](#) or [organisation](#):

- To the extent allowed by applicable law, you'll [indemnify](#) Google and its directors, officers, employees and contractors for any third-party legal proceedings (including actions by government authorities) arising out of or relating to your unlawful use of the [services](#) or breach of these terms or [service-specific additional terms](#). This indemnity covers any liability or expense arising from claims, losses, damages, judgments, fines, litigation costs and legal fees.
- If you're legally exempt from certain responsibilities, including [indemnification](#), then those responsibilities don't apply to you under these terms. For example, the United Nations enjoys certain immunities from legal obligations and these terms don't override those immunities.

Taking action in case of problems

Before taking action as described below, we'll provide you with advance notice when reasonably possible, describe the reason for our action and give you an opportunity to fix the problem, unless doing so would:

- cause harm or [liability](#) to a user, third party or Google
- violate the law or a legal enforcement authority's order
- compromise an investigation

- compromise the operation, integrity or security of our [services](#)

Removing your content

If any of [your content](#) (1) breaches these terms, [service-specific additional terms or policies](#), (2) violates applicable law or (3) could harm our users, third parties or Google, then we reserve the right to take down some or all of that content in accordance with applicable law. Examples include child pornography, content that facilitates human trafficking or harassment, terrorist content and content that infringes someone else's [intellectual property rights](#).

Suspending or terminating your access to Google services

Google reserves the right to suspend or terminate your access to the services or delete your Google Account if any of these things happen:

- you materially or repeatedly breach these terms, [service-specific additional terms or policies](#)
- we're required to do so to comply with a legal requirement or a court order
- your conduct causes harm or [liability](#) to a user, third party or Google – for example, by hacking, phishing, harassing, spamming, misleading others or scraping content that doesn't belong to you

For more information about why we disable accounts and what happens when we do, see this [Help Centre page](#). If you believe that your Google Account has been suspended or terminated in error, [you can appeal](#).

Of course, you're always free to stop using our services at any time. If you do stop using a service, we'd [appreciate knowing why](#) so that we can continue improving our services.

Settling disputes, governing law and courts

For information about how to contact Google, please visit our [contact page](#).

Californian law will govern all disputes arising out of or relating to these terms, [service-specific additional terms](#) or any related [services](#), regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

About these terms

By law, you have certain rights that can't be limited by a contract like these Terms of Service. These terms are in no way intended to restrict those rights.

These terms describe the relationship between you and Google. They don't create any legal rights for other people or [organisations](#), even if others benefit from that relationship under these terms.

We want to make these terms easy to understand, so we've used examples from our [services](#). But not all the services mentioned may be available in your country.

If these terms conflict with the [service-specific additional terms](#), the additional terms will govern for that service.

If it turns out that a particular term is not valid or enforceable, this will not affect any other terms.

If you don't follow these terms or the [service-specific additional terms](#), and we don't take action right away, that doesn't mean we're giving up any rights that we may have, such as taking action in the future.

We may update these terms and [service-specific additional terms](#) (1) to reflect changes in our services or how we do business – for example, when we add new services, features, technologies, pricing or benefits (or remove old ones), (2) for legal, regulatory or security reasons or (3) to prevent abuse or harm.

If we materially change these terms or [service-specific additional terms](#), we'll provide you with reasonable advance notice and the opportunity to review the changes, except (1) when we launch a new service or feature, or (2) in urgent situations, such as preventing ongoing abuse or responding to legal requirements. If you don't agree to the new terms, you should remove [your content](#) and stop using the services. You can also end your relationship with us at any time by closing your Google Account.

DEFINITIONS

affiliate

An entity that belongs to the Google group of companies, which means Google LLC and its subsidiaries, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google

Commerce Limited and Google Dialer Inc.

business user

An individual or entity who is not a consumer (see consumer).

consumer

An individual who uses Google services for personal, non-commercial purposes outside of their trade, business, craft or profession. (See business user)

copyright

A legal right that allows the creator of an original work (such as a blog post, photo or video) to decide if and how that original work may be used by others, subject to certain limitations and exceptions (such as 'fair use' and 'fair dealing').

disclaimer

A statement that limits someone's legal responsibilities.

indemnify or indemnity

An individual or organisation's contractual obligation to compensate the losses suffered by another individual or organisation from legal proceedings such as lawsuits.

intellectual property rights (IP rights)

Rights over the creations of a person's mind, such as inventions (patent rights); literary and artistic works (copyright); designs (design rights), and symbols, names and images used in commerce (trademarks). IP rights may belong to you, another individual or an organisation.

liability

Losses from any type of legal claim, whether the claim is based on a contract, tort (including negligence) or other reason, and whether or not those losses could have been reasonably anticipated or foreseen.

organisation

A legal entity (such as a corporation, non-profit or school) and not an individual person.

services

The Google services that are subject to these terms are the products and services listed at <https://policies.google.com/terms/service-specific>, including:

- apps and sites (like Search and Maps)
- platforms (like Google Shopping)
- integrated services (such as Maps embedded in other companies' apps or sites)
- devices and other goods (like Google Nest)

Many of these services also include content that you can stream or interact with.

trademark

Symbols, names and images used in commerce that are capable of distinguishing the goods or services of one individual or organisation from those of another.

warranty

An assurance that a product or service will perform to a certain standard.

your content

Things that you create, upload, submit, store, send, receive or share using our services, such as:

- Docs, Sheets and Slides that you create
- blog posts that you upload through Blogger
- reviews that you submit via Maps
- videos that you store in Drive
- emails that you send and receive through Gmail
- pictures that you share with friends via Photos
- travel itineraries that you share with Google

EXHIBIT 139

3/31/20 Chrome Terms of Service

Chrome



Google Chrome and Chrome OS Additional Terms of Service

By using Chrome or Chrome OS, you agree to the Google Terms of Service located at <https://policies.google.com/terms> and these Google Chrome and Chrome OS Additional Terms of Service.

These Google Chrome and Chrome OS Additional Terms of Service apply to the executable code version of Chrome and Chrome OS. Most source code for Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

Your use of certain components of Chrome and Chrome OS is subject to the following terms:

AVC

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Adobe

Google Chrome may include one or more components provided by Adobe Systems Incorporated and Adobe Software Ireland Limited (collectively "Adobe"). Your use of the Adobe software as provided by Google ("Adobe Software") is subject to the following additional terms (the "Adobe Terms"). You, the entity receiving the Adobe Software, will be hereinafter referred to as "Sublicensee."

1. License Restrictions.

(a) Flash Player, Version 10.x is designed only as a browser plug-in. Sublicensee may not modify or distribute this Adobe Software for use as anything but a browser plug-in for playing back content on a web page. For example, Sublicensee will not modify this Adobe Software in order to allow interoperation with applications that run outside of the browser (e.g., standalone applications, widgets, device UI).

(b) Sublicensee will not expose any APIs of the Flash Player, Version 10.x through a browser plug-in interface in such a way that allows such extension to be used to playback content from a web page as a stand-alone application.

(c) The Chrome-Reader Software may not be used to render any PDF or EPUB documents that utilize digital rights management protocols or systems other than Adobe DRM.

(d) Adobe DRM must be enabled in the Chrome-Reader Software for all Adobe DRM protected PDF and EPUB documents.

(e) The Chrome-Reader Software may not, other than as explicitly permitted by the technical specifications, disable any capabilities provided by Adobe in the Adobe Software, including but not limited to, support for PDF and EPUB formats and Adobe DRM.

2. Electronic Transmission. Sublicensee may allow the download of the Adobe Software from a web site, the Internet, an intranet, or similar technology (an, "Electronic Transmissions") provided that Sublicensee agrees that any distributions of the Adobe Software by Sublicensee, including those on CD-ROM, DVD-ROM or other storage media and Electronic Transmissions, if expressly permitted, shall be subject to reasonable security measures to prevent unauthorized use. With relation to Electronic Transmissions approved hereunder, Sublicensee agrees to employ any reasonable use restrictions set by Adobe, including those related to security and/or the restriction of distribution to end users of the Sublicensee Product.

3. EULA and Distribution Terms.

(a) Sublicensee shall ensure that the Adobe Software is distributed to end users under an enforceable end user license agreement, in favor of Sublicensee and its suppliers containing at least each of the following minimum terms (the "End-User License"): (i) a prohibition against distribution and copying, (ii) a prohibition against modifications and derivative works, (iii) a prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Adobe

Software to a human-perceivable form, (iv) a provision indicating ownership of Sublicensee Product (as defined in Section 8) by Sublicensee and its licensors, (v) a disclaimer of indirect, special, incidental, punitive, and consequential damages, and (vi) other industry standard disclaimers and limitations, including, as applicable: a disclaimer of all applicable statutory warranties, to the full extent allowed by law.

(b) Sublicensee shall ensure that the Adobe Software is distributed to Sublicensee's distributors under an enforceable distribution license agreement, in favor of Sublicensee and its suppliers containing terms as protective of Adobe as the Adobe Terms.

4. Opensource. Sublicensee will not directly or indirectly grant, or purport to grant, to any third party any rights or immunities under Adobe's intellectual property or proprietary rights that will subject such intellectual property to an open source license or scheme in which there is or could be interpreted to be a requirement that as a condition of use, modification and/or distribution, the Adobe Software be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable at no charge. For clarification purposes, the foregoing restriction does not preclude Sublicensee from distributing, and Sublicensee will distribute the Adobe Software as bundled with the Google Software, without charge.

5. Additional Terms. With respect to any update, upgrade, new versions of the Adobe Software (collectively "Upgrades") provided to Sublicensees, Adobe reserves the right to require additional terms and conditions applicable solely to the Upgrade and future versions thereof, and solely to the extent that such restrictions are imposed by Adobe on all licensees of such Upgrade. If Sublicensee does not agree to such additional terms or conditions, Sublicensee will have no license rights with respect to such Upgrade, and Sublicensee's license rights with respect to the Adobe Software will terminate automatically on the 90th day from the date such additional terms are made available to Sublicensee.

6. Proprietary Rights Notices. Sublicensee shall not, and shall require its distributors not to, delete or in any manner alter the copyright notices, trademarks, logos or related notices, or other proprietary rights notices of Adobe (and its licensors, if any) appearing on or within the Adobe Software or accompanying materials.

7. Technical Requirements. Sublicensee and its distributors may only distribute Adobe Software and/or Upgrade on devices that (i) meet the technical specifications posted on <http://www.adobe.com/mobile/licensees>, (or a successor web site thereto), and (ii) has been verified by Adobe as set forth below.

8. Verification and Update. Sublicensee must submit to Adobe each Sublicensee product (and each version thereof) containing the Adobe Software and/or Upgrade ("Sublicensee Product") that do not meet the Device Verification exemption criteria to be communicated by Google, for Adobe to verify. Sublicensee shall pay for each submission made by Sublicensee by procuring verification packages at Adobe's then-current terms set forth at <http://flashmobile.adobe.com/>. Sublicensee Product that has not passed verification may not be distributed. Verification will be accomplished in accordance with Adobe's then-current process described at <http://flashmobile.adobe.com/> ("Verification").

9. Profiles and Device Central. Sublicensee will be prompted to enter certain profile information about the Sublicensee Products either as part of the Verification process or some other method, and Sublicensee will provide such information, to Adobe. Adobe may (i) use such profile information as reasonably necessary to verify the Sublicensee Product (if such product is subject to Verification), and (ii) display such profile information in "Adobe Device Intelligence system," located at <https://devices.adobe.com/partnerportal/>, and made available through Adobe's authoring and development tools and services to enable developers and end users to see how content or applications are displayed in Sublicensee Products (e.g. how video images appear in certain phones).

10. Export. Sublicensee acknowledges that the laws and regulations of the United States restrict the export and re-export of commodities and technical data of United States origin, which may include the Adobe Software. Sublicensee agrees that it will not export or re-export the Adobe Software, without the appropriate United States and foreign governmental clearances, if any.

11. Technology Pass-through Terms.

(a) Except pursuant to applicable permissions or agreements therefor, from or with the applicable parties, Sublicensees shall not use and shall not allow the use of, the Adobe Software for the encoding or decoding of mp3 audio only (.mp3) data on any non-pc device (e.g., mobile phone or set-top box), nor may the mp3 encoders or decoders contained in the Adobe Software be used or accessed by any product other than the Adobe Software. The Adobe Software may be used for the encoding or decoding of MP3 data contained within a swf or flv file, which contains video, picture or other data. Sublicensee shall acknowledge that use of the Adobe Software for non-PC devices, as described in the prohibitions in this section, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe nor Sublicensee has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Sublicensee requires an MP3 encoder or decoder for such use, Sublicensee is responsible for obtaining the necessary intellectual property license, including any applicable patent rights.

(b) Sublicensee will not use, copy, reproduce and modify (i) the On2 source code (provided hereunder as a component of the Source Code) as necessary to enable the Adobe Software to decode video in the Flash video file format (.flv or .f4v), and (ii) the Sorenson Spark source code (provided hereunder as a component of the Source Code) for the limited purpose of making bug fixes and performance enhancements to the Adobe Software. All codecs provided with the Adobe Software may only be used and distributed as an integrated part of the Adobe Software and may not be accessed by any other application, including other Google applications.

(c) The Source Code may be provided with an AAC codec and/or HE-AAC codec ("the AAC Codec"). Use of the AAC Codec is conditioned on Sublicensee obtaining a proper patent license covering necessary patents as provided by VIA

(d) THE SOURCE CODE MAY CONTAIN CODE LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. See <http://www.mpegla.com>

12. Update. Sublicensee will not circumvent Google's or Adobe's efforts to update the Adobe Software in all Sublicensee's products incorporating the Adobe Software as bundled with the Google Software ("Sublicensee Products").

13. Attribution and Proprietary Notices. Sublicensee will list the Adobe Software in publicly available Sublicensee Product specifications and include appropriate Adobe Software branding (specifically excluding the Adobe corporate logo) on the Sublicensee Product packaging or marketing materials in a manner consistent with branding of other third party products contained within the Sublicensee Product.

14. No Warranty. THE ADOBE SOFTWARE IS MADE AVAILABLE TO SUBLICENSEE FOR USE AND REPRODUCTION "AS IS" AND ADOBE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. ADOBE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS OBTAINED BY USING THE ADOBE SOFTWARE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO SUBLICENSEE IN SUBLICENSEE'S JURISDICTION, ADOBE AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. SUBLICENSEE AGREES THAT SUBLICENSEE SHALL NOT MAKE ANY WARRANTY, EXPRESS OR IMPLIED, ON BEHALF OF ADOBE.

15. Limitation of Liability. IN NO EVENT WILL ADOBE OR ITS SUPPLIERS BE LIABLE TO SUBLICENSEE FOR ANY DAMAGES, CLAIMS OR COSTS WHATSOEVER OR ANY CONSEQUENTIAL, INDIRECT, OR INCIDENTAL DAMAGES, OR ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ADOBE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, DAMAGES, CLAIMS OR COSTS OR FOR ANY CLAIM BY ANY THIRD PARTY. THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW IN SUBLICENSEE'S JURISDICTION. ADOBE'S AGGREGATE LIABILITY AND THAT OF ITS SUPPLIERS UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO ONE THOUSAND DOLLARS (US\$1,000). Nothing contained in this Agreement limits Adobe's liability to Sublicensee in the event of death or personal injury resulting from Adobe's negligence or for the tort of deceit (fraud). Adobe is acting on behalf of its suppliers for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose.

16. Content Protection Terms

(a) Definitions.

"Compliance and Robustness Rules" means the document setting forth compliance and robustness rules for the Adobe Software located at <http://www.adobe.com/mobile/licensees>, or a successor web site thereto.

"Content Protection Functions" means those aspects of the Adobe Software that are designed to ensure compliance with the Compliance and Robustness Rules, and to prevent playback, copying, modification, redistribution or other actions with respect to digital content distributed for consumption by users of the Adobe Software when such actions are not authorized by the owners of such digital content or its licensed distributors.

"Content Protection Code" means code within certain designated versions of the Adobe Software that enables certain Content Protection Functions.

"Key" means a cryptographic value contained in the Adobe Software for use in decrypting digital content.

(b) License Restrictions. Sublicensee's right to exercise the licenses with respect to the Adobe Software is subject to the following additional restrictions and obligations. Sublicensee will ensure that Sublicensee's customers comply with these restrictions and obligations to the same extent imposed on Sublicensee with respect to the Adobe Software; any failure by Sublicensee's customers to comply with these additional restrictions and obligations shall be treated as a material breach by Sublicensee.

b.1. Sublicensee and customers may only distribute the Adobe Software that meets the Robustness and Compliance Rules as so confirmed by Sublicensee during the verification process described above in the Adobe Terms.

b.2. Sublicensee shall not (i) circumvent the Content Protection Functions of either the Adobe Software or any related Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software or (ii) develop or distribute products that are designed to circumvent the Content Protection Functions of either the Adobe Software or any Adobe Software that is used to encrypt or decrypt digital content for authorised consumption by users of the Adobe Software.

(c) The Keys are hereby designated as Adobe's Confidential Information, and Sublicensee will, with respect to the Keys, adhere to Adobe's Source Code Handling Procedure (to be provided by Adobe upon request).

(d) Injunctive Relief. Sublicensee agrees that a breach of this Agreement may compromise the Content Protection Functions of the Adobe Software and may cause unique and lasting harm to the interests of Adobe and owners of digital content that rely on such Content Protection Functions, and that monetary damages may be inadequate to compensate fully for such harm. Therefore, Sublicensee further agrees that Adobe may be entitled to seek injunctive relief to prevent or limit the harm caused by any such breach, in addition to monetary damages.

17. **Intended Third-party Beneficiary.** Adobe Systems Incorporated and Adobe Software Ireland Limited are the intended third-party beneficiaries of Google's agreement with Sublicensee with respect to the Adobe Software, including but not limited to, the Adobe Terms. Sublicensee agrees, notwithstanding anything to the contrary in its agreement with Google, that Google may disclose Sublicensee's identity to Adobe and certify in writing that Sublicensee has entered into a license agreement with Google which includes the Adobe Terms. Sublicensee must have an agreement with each of its licensees, and if such licensees are allowed to redistribute the Adobe Software, such agreement will include the Adobe Terms.

Additionally, your use of certain components of Chrome OS is subject to the following terms:

MPEG-4

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

EXHIBIT 140

1/1/21 Chrome Terms of Service



Google Chrome and ChromeOS Additional Terms of Service

Last modified: 01 January, 2021

By using Chrome or ChromeOS, you agree to the Google Terms of Service located at <https://policies.google.com/terms> and these Google Chrome and ChromeOS Additional Terms of Service.

These Google Chrome and ChromeOS Additional Terms of Service apply to the executable code version of Chrome and ChromeOS. Most source code for Chrome is available free of charge under open source software license agreements at <https://code.google.com/chromium/terms.html>.

Your use of certain components of Chrome and ChromeOS is subject to the following terms:

AVC

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Additionally, your use of certain components of ChromeOS is subject to the following terms:

MPEG-4

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

English - United States

EXHIBIT 141

2/2/2021 GOOGLE CHROME PRIVACY WHITEPAPER

Google Chrome Privacy Whitepaper

Last modified: February 4, 2021 (Current as of Chrome 87.0.4280.141)

- [Omnibox](#)
- [Network predictions](#)
- [Search locale](#)
- [New Tab page](#)
- [Touch to Search](#)
- [Search with Google Lens](#)
- [Safe Browsing protection](#)
- [Safety Check](#)
- [Unwanted software protection](#)
- [Offline Indicator](#)
- [Google update](#)
- [Network time](#)
- [Counting install](#)
- [Measuring promotions](#)
- [Usage stats](#)
- [Google Surveys](#)
- [Spelling suggestions](#)
- [Translate](#)
- [Image Descriptions](#)

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

[Ok, got it](#)

-
- [Google Assistant on Android devices](#)
 - [Cloud Print](#)
 - [SSL certificate error reporting](#)
 - [Installed apps](#)
 - [Push Messaging](#)
 - [Chrome custom tabs](#)
 - [Continue where you left off](#)
 - [Chrome variations](#)
 - [Do Not Track](#)
 - [Plugins](#)
 - [Media licenses](#)
 - [MediaDrm provisioning](#)
 - [Cloud policy](#)
 - [Lite Mode \(Chrome mobile\)](#)
 - [Kid's Google Account](#)
 - [Incognito and Guest mode](#)
 - [Handoff support](#)
 - [Security key](#)
 - [Physical web](#)
 - [Bluetooth](#)
 - [Data sent by Android](#)
 - [Integration with Digital Wellbeing](#)

This document describes the features in Chrome that communicate with Google, as well as with third-party services (for example, if you've changed your default search engine). This document also describes the controls available to you regarding how your data is used by Chrome. [Here](#)

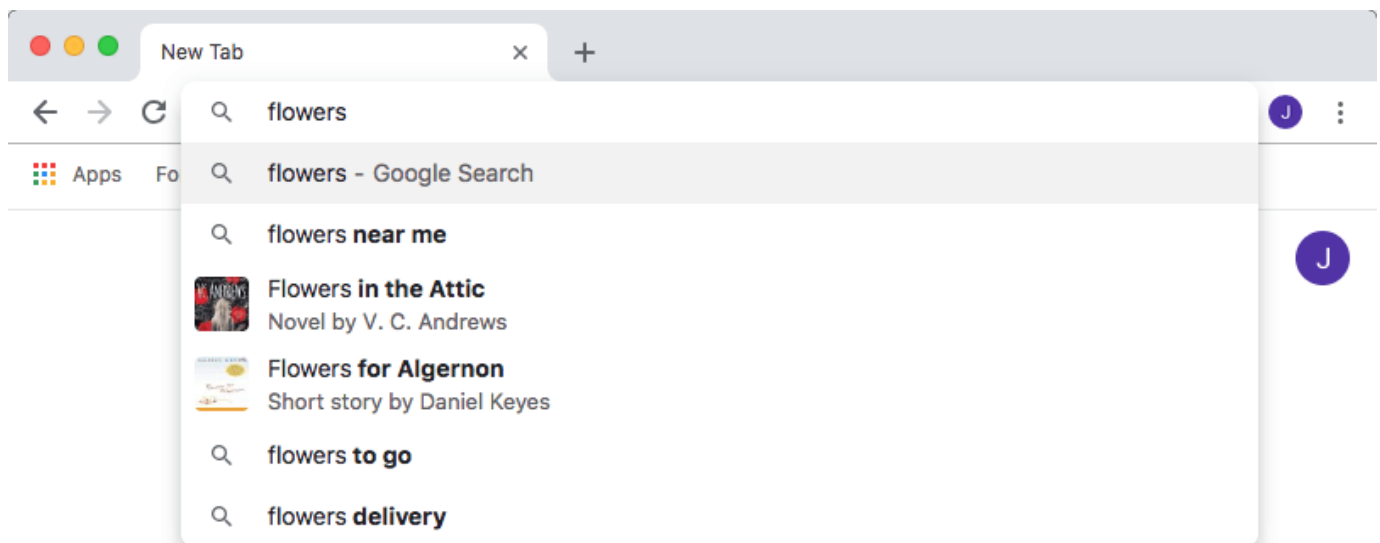
Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

file it in [our public bug tracker](#). For issues that include confidential information, please use [this link](#). We'd be happy to hear from you.

Omnibox

Google Chrome uses a combined [web address and search bar](#) (we call it the "omnibox") at the top of the browser window.

As you use the omnibox, your [default search engine](#) can suggest addresses and search queries that may be of interest to you. These suggestions make navigation and searching faster and easier, and are turned on by default. They can be turned off by unchecking "Autocomplete searches and URLs" in the "Sync and Google services" section of Chrome's settings.



When not in Incognito mode, in order to provide these suggestions, Chrome sends the text you've typed into the omnibox, along with a general categorization (e.g., "URL", "search query", or "unknown"), to your default search engine. Chrome will also send a signal to your default search engine when you focus in the omnibox, telling it to get ready to provide suggestions. That signal

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

"Preload pages for faster browsing and searching" in the "Cookies" part of "Privacy and security" section or "Autocomplete searches and URLs" in the "Sync and Google services" section of Chrome's settings. When Chrome preconnects, it resolves the search engine's IP address and connects it to the search engine, exposing your IP address.

When in Incognito mode, in order to provide these suggestions, Chrome relies on an on-device model that does not communicate with your default search engine until you select a suggestion.

If Chrome determines that your typing may contain sensitive information, such as authentication credentials, local file names, or URL data that is normally encrypted, it will not send the typed text.

If Google is your default search engine, when you select one of the omnibox suggestions, Chrome sends your original search query, the suggestion you selected, and the position of the suggestion back to Google. This information helps improve the quality of the suggestion feature, and it's logged and anonymized in the same manner as Google web searches. Logs of these suggestion requests are retained for two weeks, after which 2%% of the log data is randomly selected, anonymized, and retained in order to improve the suggestion feature.

If you've chosen to sync your Chrome history, and if Google is your default search engine, the URL of the page you're viewing is sent to Google in order to provide better, contextually relevant suggestions. URLs are sent only for HTTP pages and HTTPS pages, not other schemes such as file: and ftp:. Additionally, Chrome may present website and search query suggestions as soon as you place the cursor in the omnibox, before you start typing. Chrome is in the process of transitioning to a new service to provide these on-focus suggestions. For most users on desktop versions of Chrome, the request and complete set of suggestions are retained on Google servers in order to further improve and personalize the feature. When the URL that triggered the set of

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

you haven't blocked geolocation for www.google.com (or country-specific origins such as www.google.de). Additionally, if your device has network location enabled (High Accuracy or Battery Saving Device Location mode in Android settings), the X-Geo header may also include visible network IDs (WiFi and Cell), used to geocode the request server-side. The X-Geo header will never be sent in Incognito mode. HTTPS will be required to include this header in the request. You can learn more about how to control the Android OS location sharing with apps on [this article](#) for Nexus, or find your device [here](#) if you do not use a Nexus. How to control location sharing with a site within Chrome is written in [this article](#). See the [Geolocation](#) section of this whitepaper for more information on default geolocation permissions.

Additionally, if Google is your default search engine and you have enabled sync, omnibox may also show suggestions for your Google Drive files. You can turn this functionality off by disabling the "Drive suggestions" option in the "Sync and Google services" section of Chrome's settings.

If you use a non-Google search provider as your default search engine, queries are sent and logged under that provider's privacy policy.

Additionally, when you use the omnibox to search for a single word, Chrome may send this word to your DNS server to see whether it corresponds to a host on your network, and may try to connect to the corresponding host. This gives you the option to navigate to that host instead of searching. For example, if your router goes by the hostname "router", and you type "router" in the omnibox, you're given the option to navigate to <https://router/>, as well as to search for the word "router" with your default search provider. This feature is not controlled by the "Use a prediction service to help complete searches and URLs..." option because it does not involve sending data to your default search engine.

Network predictions

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

and TLS preconnection, and prefetching of web pages. To [turn off](#) network predictions, uncheck “Preload pages for faster browsing and searching” in the “Privacy and security > Cookies” section of Chrome’s settings on desktop, in the “Privacy” section of Chrome’s settings on Android, and in the “Bandwidth” section of Chrome’s settings on iOS.

To improve load times, the browser can be asked to prefetch links that you might click next. Chrome supports five types of prefetching:

- Chrome prefetching - can be initiated by Chrome itself whenever it detects a search query typed in the omnibox, a likely beginning of a URL you type often in the omnibox, or when you have [Lite mode](#) enabled and are visiting Google Search.
- Webpage prefetching - requested by one web page to prefetch another
- AMP prefetching - can be requested only by the Google Search App on Android to prefetch several accelerated mobile pages (AMP) articles and display them later in a Chrome Custom Tab
- CustomTabs prefetching - any Android app can request to prefetch several URLs to speed up displaying them later in a Chrome Custom Tab
- Privacy-preserving search result link prefetching - can be initiated by Chrome on Google Search result pages to prefetch links to other websites.

Four mechanisms preserve user privacy for search result link prefetches:

- Prefetching is restricted to domains for which Chrome doesn’t have a corresponding cookie.
- Passive fingerprinting surfaces such as User-Agent are bucketed or set to fixed values.
- Prefetches are limited to HTTPS links and tunneled through a [CONNECT](#) proxy operated by Google. Consequently, the TLS connection is established between Chrome and the

Controlling the feature. All prefetching types except webpage prefetching are controlled by Chrome's prediction service setting. Webpage prefetching is allowed regardless of whether Chrome's network prediction service feature is enabled.

Handling of cookies. Except for the privacy-preserving search result link prefetching case, the prefetched site is allowed to set and read its own cookies even if you don't end up visiting the prefetched page, and prefetching is disabled if you have chosen to block third-party cookies. In the privacy-preserving search result link prefetching case, prefetching is disabled if you have a cookie for the site, and the site can only set a cookie once you click on the link that was prefetched.

Javascript execution. For AMP prefetching the page is fully rendered and Javascript is also executed. For the remaining types of prefetching Javascript is not executed.

Google search locale

If Google is set as your default search engine, Chrome will try to determine the most appropriate locale for Google search queries conducted from the [omnibox](#) in order to give you relevant search results based on your location. For example, if you were in Germany, your omnibox searches may go through google.de instead of google.com.

In order to do this, Chrome will send a request to google.com each time you start the browser. If you already have any cookies from the google.com domain, this request will also include these cookies, and is logged as any normal HTTPS request to google.com would be (see the [description of "server logs" in the privacy key terms](#) for details). If you do not have any cookies from google.com, this request will not create any.

New Tab page

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

of the sites you visited may also be sent to Google to provide suggestions in languages you prefer to read, and the device display DPI may be sent to format content for your device. To save data, Chrome may additionally send a hash of the content that Google provided to you the last time, so that you only download content when there is something new.

If you are signed into Chrome, suggestions are *also* based on data stored in your Google account activity. You can control the collection of data in your Google account at [Activity controls](#) and manage your account activity at [My Activity](#). For example, if you sync your browsing history and have enabled its use in your Web & App activity, Google may suggest sites that relate to sites you have visited in the past. Chrome measures the quality of suggestions by sending Google information about the sets of suggestions that were displayed, and those that were selected.

On the desktop version of Chrome, you may also manually add shortcuts to websites that you regularly visit, or edit Chrome's existing website suggestions. After you add, edit, or delete a shortcut to a website, the Chrome New Tab page will not suggest any new websites to you.

Suggestions generated from your browsing history will be removed once you clear your browsing history. However, if you customized your suggestions, they will not be removed.

For Chrome on Android, in certain countries, Chrome may download the content of the New Tab page suggestions from Google, for use while offline. Chrome sends to Google a cookieless request with the URL for each suggestion, along with Chrome's user agent string, in order to render the content. You can remove downloaded content by clearing Chrome's cache data, or by opening the Downloads menu and [selecting individual pages to delete](#). You can disable this feature by disabling "Download articles for you on Wi-Fi" in Chrome's Downloads settings.

On mobile versions of Chrome, if you're signed in to Chrome and have the [Web & App activity](#) setting enabled for your account, your preferences for the suggested articles can be modified or

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

on or ignoring an article). You can manage this interaction data, which is stored in the Discover section of your Google account, at [My Activity](#). Google may use anonymized and aggregated interest and interaction data from you to improve the quality of suggested articles for other users. For instance, if you view or open a suggestion it might be suggested more often, while if you report its contents as inappropriate it might stop being suggested.

For desktop and Android versions of Chrome, when you open a new tab, Chrome loads a New Tab page customized by your default search engine (e.g., google.com) if it's available. This page is preloaded in the background and refreshed periodically so that it opens quickly. Your IP address and cookies, as well as your current browser theme, are sent to your search engine with each refresh request so that the New Tab page can be correctly displayed. See the [Embedded Search API](#) for more details. Your search engine may also record your interactions with the New Tab page.

The New Tab page content may be designed by your default search provider. Suggested websites are embedded by Chrome into the New Tab page in a way that does not expose them to your default search provider.

If your default search provider is Google, the New Tab page also contains a web address and search bar that behaves like the [omnibox](#).

This information about the New Tab page may not apply if you've installed an extension that [overrides the New Tab page](#).

Touch to Search

If you've enabled "Touch to Search" on Chrome Mobile you can search for terms by selecting them.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

searches and browsing better”, the URL of the page is also sent and logged, and is used to improve your query suggestions.

When Google returns a search suggestion, a card appears that may present an action or additional information related to the search. Opening this card is considered a regular search and navigation on Google, so standard logging policies apply.

Adjusting a selection causes a search for the exact selection. For example, if the user selects "climate" and the selection is automatically expanded to "climate change", the user can adjust the selection back to just "climate" and opening the panel would show full search results for "climate" rather than "climate change". Saying "Ok Google" after selecting a word provides the word and its surrounding text as context for the Google Assistant.

Touch to Search is enabled in a limited mode by default: potentially privacy-sensitive data, such as the URL and surrounding text, is not sent for HTTPS pages. Touch to Search can be fully enabled and disabled in the card or in the Chrome privacy settings.

Search with Google Lens

On Android Chrome, if Google is selected as the default search engine and a recent version of the Google app is installed on your device, touching & holding on an image will present you with an option to initiate a search with Google Lens.

A tap on that menu item will redirect you to the Lens experience in the Google App and the image bytes of the selected image will be sent to the Google Lens app. For non-incognito users, the name of the currently signed-in account (if applicable), image tag attributes, and Chrome [experiments](#) may also be sent to the Google App. This information is used to improve the user experience within the Lens app.

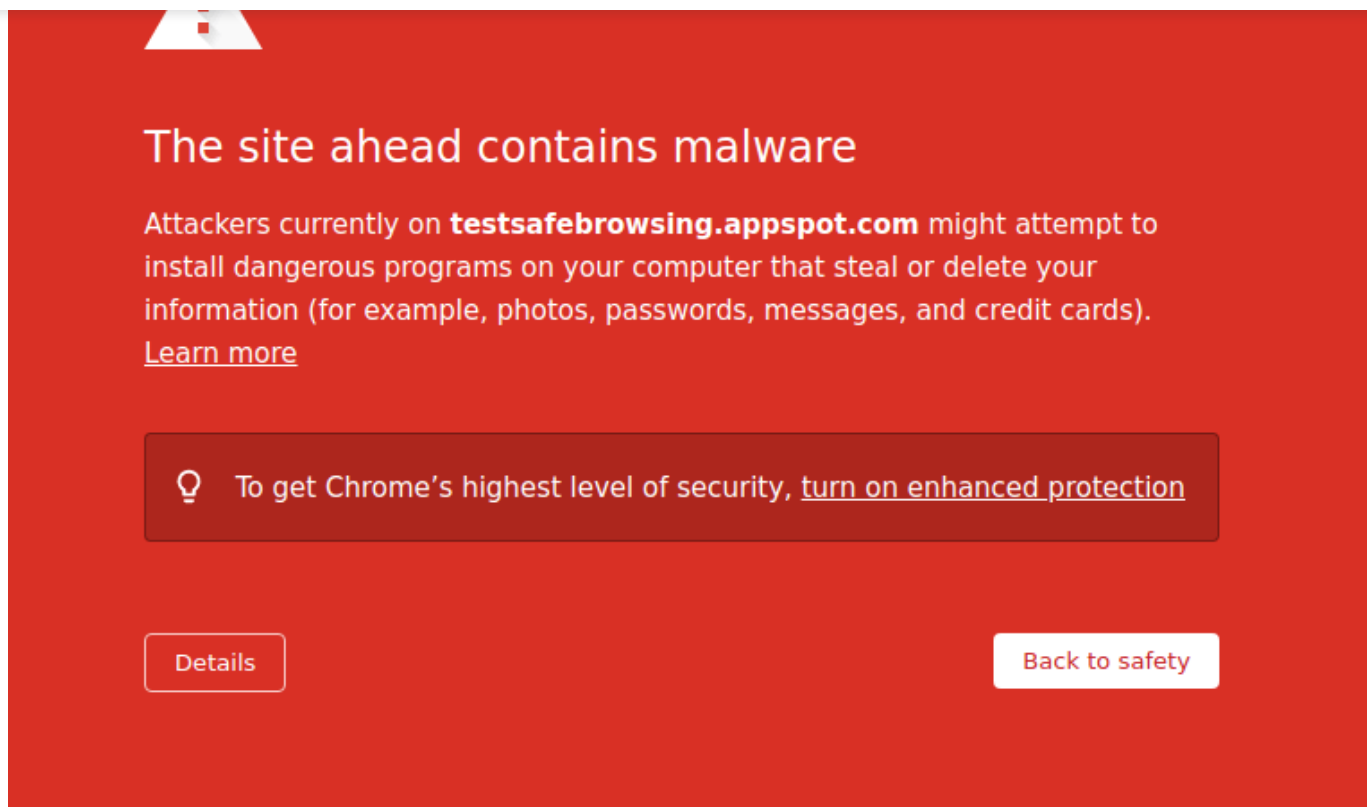
Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

abusive websites or extensions. You can find more information at safebrowsing.google.com about how Safe Browsing protects you in Chrome and other Google products. Safe Browsing is designed specifically to protect your privacy and is also used by other popular browsers.

You can find settings for Safe Browsing in the “Privacy and security > Security” section of Chrome’s settings. When Safe Browsing is enabled in the “Standard protection” mode (pictured below), Chrome contacts Google’s servers periodically to download the most recent Safe Browsing list of unsafe sites including sites associated with phishing, social engineering, malware, unwanted software, malicious ads, intrusive ads, and abusive websites or Chrome extensions. The most recent copy of this list is stored locally on your system. Chrome checks the URL of each site you visit or file you download against this local list. If you navigate to a URL that appears on the list, Chrome sends a partial URL fingerprint (the first 32 bits of a SHA-256 hash of the URL) to Google for verification that the URL is indeed dangerous. Chrome also sends a partial URL fingerprint when a site requests a potentially dangerous permission, so that Google can protect you if the site is malicious. Google cannot determine the actual URL from this information.

In addition to the URL check described above, Chrome also conducts client-side checks. If a website looks suspicious, Chrome sends a subset of likely phishing and social engineering terms found on the page to Google, in order to determine whether the website should be considered malicious. These client-side checks also include comparisons of the visual appearance of the page to a list of images of login pages. If a website appears similar to a page on this list, Chrome will send the URL and the matched entry on the list to Google to determine whether the page is a likely phishing attempt. Chrome can also help protect you from phishing if you type one of your previously saved passwords into an uncommon site. In this case Chrome sends the URL and referrers of the page to Google to see if the page might be trying to steal your password.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).



You can [visit our malware warning test page](#) or [social engineering warning test page](#) to see the above example in action. For more information about the warning pages, see [Manage warnings about unsafe sites](#).

Additionally, if you've opted into "Make Searches and Browsing Better (sends URLs of the pages you visit to Google)", Chrome sends a request to Safe Browsing each time you visit a page that isn't in Chrome's local list of safe sites in order to gather the latest reputation of that website (we call this mechanism "real-time checks"). If you sync your browsing history without a sync passphrase, this request also contains a temporary authentication token tied to your Google account to provide better protections to some users whose account may be under attack. If the website is deemed unsafe by Safe Browsing, you may see a warning like the one shown above.

This mechanism is designed to catch unsafe sites that switch domains very quickly or hide from

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

an incident report to Google every time you receive a warning, visit a suspicious page, and on a very small fraction of sites where Chrome thinks there could be threats, to help Safe Browsing learn about the new threats you may be encountering. Additionally, some downloaded files that are suspicious and show a warning may be sent to Google for investigation each time they are encountered. All reports are sent to Google over an encrypted channel and can include URLs, headers, and snippets of content from the page and they never include data from browsing you do in Incognito mode. If Chrome discovers unwanted or malicious software on your machine, the reports may also include details about malicious files and registry entries. This data is used only to improve Safe Browsing and to improve security on the Internet. For example, Chrome reports some [SSL certificate](#) chains to Google to help improve the accuracy of Chrome's SSL warnings. As part of [Certificate Transparency](#), Chrome also reports to Google a sampling of information about SSL certificates and any observed signed certificate timestamps (SCTs). These reports help Google verify that the third-party logs in the Certificate Transparency system are behaving honestly, which helps ensure that HTTPS connections can be trusted. Chrome does not send reports for connections authenticated with certificates that chain to locally installed roots.

Please be aware that if you disable the Safe Browsing feature, Chrome will no longer be able to protect you from websites that try to steal your information or install harmful software. We don't recommend turning it off.

If you are a webmaster, developer, or network admin, you can find more relevant information about Safe Browsing on [this page](#).

Safe Browsing also protects you from abusive extensions and malicious software. When Chrome starts, and on each update of the Safe Browsing list, Chrome scans extensions installed in your browser against the Safe Browsing list. If an extension on the list is found, Chrome will disable the extension, offer you relevant information and may provide an option for you to

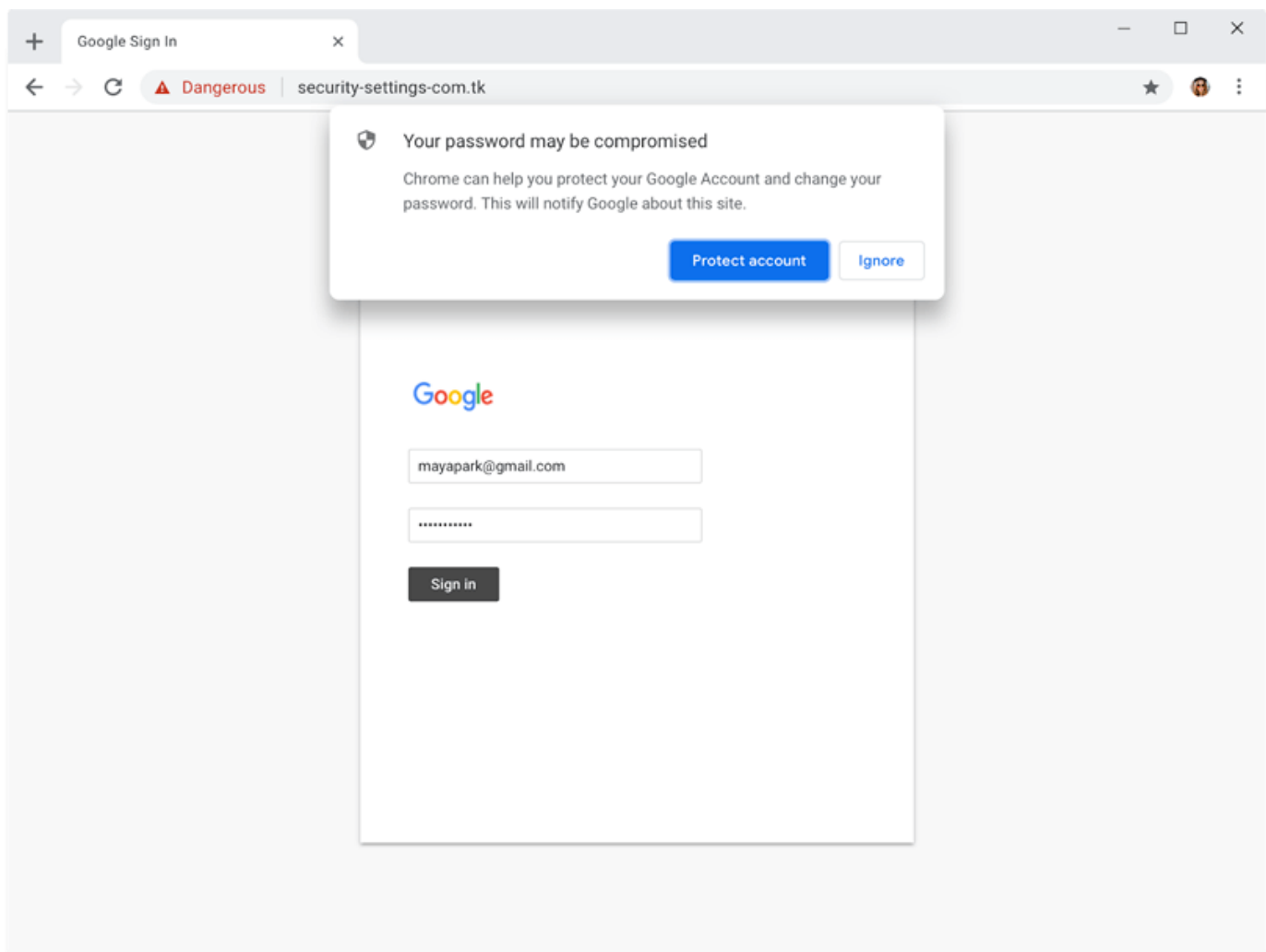
Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

To warn you about potentially dangerous files, like the picture shown above, Chrome checks the URL of potentially dangerous file types you download against a list of URLs that have been verified. Potentially dangerous file types include both executables and commonly-abused document types. This list is stored locally on your computer and updated regularly. Chrome does not send information to Google for files you download from URLs in this list, or if the file is signed by a verified publisher. For all other unverified potentially dangerous file downloads, Chrome sends Google the information needed to help determine whether the download is harmful, including some or all of the following: information about the full URL of the site or file download, all related referrers and redirects, code signing certificates, file hashes, and file header information. Chrome may then show a warning like the one pictured above.

If you are enrolled in [Google's Advanced Protection Program](#), Chrome will show you additional warnings when you download files but where Safe Browsing is unable to ascertain they are safe.

Chrome helps protect you against password phishing by checking with Google when you enter your password on an uncommon page. Chrome keeps a local list of popular websites that Safe Browsing found to be safe. If Chrome detects that you have entered your Google account password or one of your passwords stored in Chrome's password manager on a website that's not on the list, it sends a request to Safe Browsing to gather the reputation of that website. The verdict received from Safe Browsing is usually cached on your device for 1 week. For users who have enabled the "Help improve security on the web for everyone" setting, Chrome will ignore the list of popular websites for a small fraction of visits, to test the accuracy of that list.

If the reused password is your Google account password and the verdict for the website is that it is phishing, Chrome will suggest that you change your Google account password to avoid losing



If you've opted into “Help improve security on the web for everyone”, Chrome also sends a request to Safe Browsing each time you start to enter a password on a page that isn't in Chrome's local list. In addition, the request Chrome sends to Safe Browsing to determine the reputation of the website on which you reuse your password includes the list of websites for which you saved this password in Chrome's password manager (but not the password itself).

If Chrome detects that your settings have been tampered with, Chrome reports the URL of the

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

the request.



Faster, proactive protection against dangerous websites, downloads, and extensions.
Warns you about password breaches. Requires browsing data to be sent to Google.



Predicts and warns you about dangerous events before they happen



Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in



Improves security for you and everyone on the web



Warns you if passwords are exposed in a data breach



Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.

Standard protection



Standard protection against websites, downloads, and extensions that are known to be dangerous.



Detects and warns you about dangerous events when they happen



Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.

Help improve security on the web for everyone

Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.



Warn you if passwords are exposed in a data breach

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by



Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

requests for checking potentially dangerous file downloads contain a temporary authentication token tied to your Google account that is used to protect you across Google apps. Enhanced protection also enables reporting additional [data relevant to security](#) to help improve Safe Browsing and overall web security, and it enables Chrome's password breach detection. When browsing in incognito or guest mode, these extra checks do not occur, and Enhanced protection mode operates the same way as Standard protection.

For all Safe Browsing requests and reports, Google logs the transferred data in its raw form and retains this data for up to 30 days. Google collects standard log information for Safe Browsing requests, including an IP address and one or more cookies. After at most 30 days, Safe Browsing deletes the raw logs, storing only calculated data in an anonymized form that does not include your IP addresses or cookies. Additionally, Safe Browsing requests won't be associated with your Google Account, except if the request includes the temporary authentication token described above. They are, however, tied to the other Safe Browsing requests made from the same device.

For Chrome on iOS 13 and later, Apple allows for connecting to multiple Safe Browsing services. This means that Chrome may connect to a third-party Safe Browsing service instead of the Google one. Apple determines which Safe Browsing service to connect to based on factors like your device locale.

Safety Check

Google Chrome includes a Safety check feature in settings. Running the Safety check verifies whether the browser is [up to date](#), whether [Safe Browsing](#) is enabled, whether your passwords [have been exposed as a part of a data breach](#), on Desktop whether you have potentially harmful [extensions](#) installed, and on Windows whether [unwanted software](#) has been found on your

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).



Chrome can help keep you safe from data breaches, bad extensions, and more

Check now

Unwanted software protection

The Windows version of Chrome is able to detect and remove certain types of software that violate [Google's Unwanted Software Policy](#). If left in your system, this software may perform unwanted actions, such as changing your Chrome settings without your approval. Chrome periodically scans your device to detect potentially unwanted software. In addition, [if you have opted in to automatically report details of possible security incidents to Google](#), Chrome will report information about unwanted software, including relevant file metadata and system settings linked to the unwanted software found on your computer.

If you perform an unwanted software check on your computer from the Settings page, Chrome reports information about unwanted software and your system. System information includes metadata about programs installed or running on your system that could be associated with harmful software, such as: services and processes, scheduled tasks, system registry values commonly used by malicious software, command-line arguments of Chrome shortcuts, Windows proxy settings, and software modules loaded into Chrome or the network stack. You can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the scan.

If unwanted software is detected, Chrome will offer you an option to clean it up by using the Chrome Cleanup Tool. This will [quarantine](#) detected malicious files, delete harmful extensions and registry keys, and [reset](#) your settings. The Chrome Cleanup Tool also reports information about unwanted software and your system to Google, and again you can opt out of sharing this data by deselecting the checkbox next to "Report details to Google" before starting the cleanup.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

cookieless request to http://connectivitycheck.gstatic.com/generate_204 or http://clients4.google.com/generate_204 to determine whether you're offline and display an offline indicator.

Software updates

Desktop versions of Chrome and the Google Chrome Apps Launcher use [Google Update](#) to keep you up to date with the latest and most secure versions of software. In order to provide greater transparency and to make the technology available to other applications, the Google Update technology is open source.

Google Update requests include information necessary for the update process, such as the version of Chrome, its release channel, basic hardware information, and update errors that have been encountered. The update requests also send Google information that helps us understand [how many people](#) are using Google Chrome and the Chrome Apps Launcher – specifically, whether the software was used in the last day, the number of days since the last time it was used, the total number of days it has been installed, and the number of active profiles. Google Update also periodically sends a non-unique four-letter tag that contains information about [how you obtained Google Chrome](#). This tag is not personally identifiable, does not encode any information about when you obtained Google Chrome, and is the same as everyone who obtained Google Chrome the same way.

Because ChromeOS updates the entire OS stack, Google Update on ChromeOS also sends the current ChromeOS version and hardware model information to Google in order to ensure that the correct software updates and hardware manufacturer customizations such as apps, wallpaper, and help articles are delivered. This information is not personally identifiable, and is common to all users of ChromeOS on the same revision of device.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

information (such as the application ID, when the application was last used, and how long it's been installed). We use these requests to determine the aggregate popularity and usage of applications and extensions. If you are using an extension or application restricted to a certain audience, authentication tokens are sent with the update requests for these add-ons. For security reasons, Chrome also occasionally sends a cookieless request to the Chrome Web Store, in order to verify that installed extensions and applications that claim to be from the store are genuine.

In order to keep updates as small as possible, Google Chrome is internally split into a variety of components, each of which can be updated independently. Each component is uniquely identified via an ID that is shared among all Google Chrome installations (e.g., "fmeadaodfnidclnjhlkdjgkolmhmfofk"). An update request for a component contains this ID, the hash of the previous download (called a "fingerprint"), and the component's version. Because every installation has the same ID, and downloads of the same component have the same fingerprint, none of this information is personally identifiable.

If you install web apps on an Android device, a Google server is responsible for creating a native Android package that can be verified for authenticity by Chrome. When Chrome is updated or notices that the web app's manifest has changed, Chrome asks the server for a new version of the Android package in a cookieless request. If the information needed to create the native Android package cannot be acquired by the server (e.g., because the information is behind a corporate firewall), Chrome sends it to Google and an Android package is created that is unique to you. It contains a unique and random identifier that is not tied to your identity.

Chrome may also download and run a binary executable (e.g., as part of the software update or to improve Safe Browsing protection). These executables are cryptographically signed and verified before execution. Chrome may download further static resources like dictionaries on

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Network time

On desktop platforms, Chrome uses [network time](#) to verify SSL certificates, which are valid only for a specified time. At random intervals or when Chrome encounters an expired SSL certificate, Chrome may send requests to Google to obtain the time from a trusted source. These requests are more frequent if Chrome believes the system clock is inaccurate. These requests contain no cookies and are not logged on the server.

Counting installations

In order to measure the success rate of Google Chrome downloads and installations of the Windows version of Google Chrome, a randomly-generated token is included with Google Chrome's installer. This token is sent to Google during the installation process to confirm the success of that particular installation. A new token is generated for every install. It is not associated with any personal information, and is deleted once Google Chrome runs and checks for updates the first time.

For Chrome to know how many active installations it has, the mobile version of Chrome sends a ping to Google with a salted hash of a device identifier on an ongoing basis. The desktop version of Chrome does not send any stable identifier to count active installations. Instead an anonymous message to Google with a timestamp of the last ping is used to infer number of active installations.

Measuring effectiveness of a promotion

Chrome utilizes two measurements to understand how effective a promotional campaign has been: how many Chrome installations are acquired through a promotional campaign, and how much Chrome usage and traffic to Google is driven by a campaign.

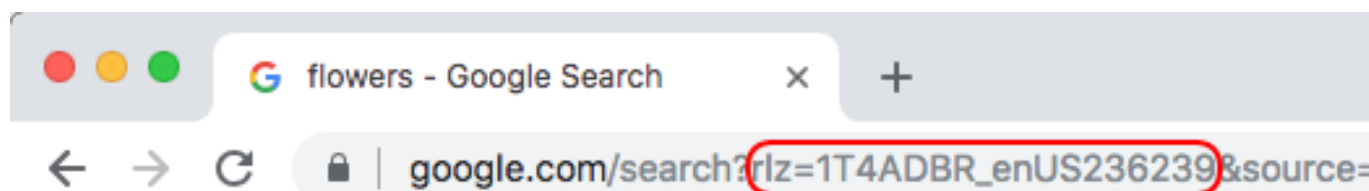
Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

computer, it is generated when necessary by using built-in system information that is scrambled in an irreversible manner. On iOS, Chrome uses the [IDFA](#) for counting installations acquired by a campaign, and it can be reset in iOS settings.

To measure searches and Chrome usage driven by a particular campaign, Chrome inserts a promotional tag, not unique to you or your device, in the searches you perform on Google. This non-unique tag contains information about how Chrome was obtained, the week when Chrome was installed, and the week when the first search was performed. For desktop versions of Chrome, Chrome generates a promotional tag, if the promotional installation token described in the previous paragraph indicates that Chrome has been installed or reactivated by a campaign on a device which has not been associated with any campaign yet. For Chrome on Mobile, a promotional tag is always sent regardless of the source of installations.

The promotional tag is generated using a software library called "RLZ" and looks similar to "1T4ADBR_enUS236US239". The RLZ library was fully open-sourced in June 2010. For more information, please see the [In the Open, for RLZ](#) post on the Chromium blog and the article ["How To Read An RLZ String"](#). On Android, this promotional tag can also be a readable string like "android-hms-tmobile-us" instead of an RLZ string, and is not unique to either you or your device.

This non-unique promotional tag is included when performing searches via Google (the tag appears as a parameter beginning with "rlz=" when triggered from the Omnibox, or as an "x-rlz-string" HTTP header). We use this information to measure the searches and Chrome usage driven by a particular promotion.




Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

regions.

For the desktop version of Chrome, you can opt-out of sending this data to Google by uninstalling Chrome, and installing a version downloaded directly from www.google.com/chrome. To opt-out of sending the RLZ string in ChromeOS, press Ctrl + Alt + T to open the [crosh shell](#), type rlz disable followed by the enter key, and then reboot your device.

Usage statistics and crash reports

Chrome has a feature to automatically send [usage statistics and crash reports](#) to Google in order to help improve Chrome's feature set and stability.

 Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. [Learn more](#)

Usage statistics contain information such as system information, preferences, user interface feature usage, responsiveness, performance, and memory usage. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs, actions taken by the user before the crash, and/or personal information depending on what was happening at the time of the crash. This feature is enabled by default for Chrome installations of version 54 or later. You can control the feature in the "Sync and Google services" section of Chrome's settings.

When this feature is enabled, Google Chrome stores a randomly generated unique token on your device, which is sent to Google along with your usage statistics and crash reports. The token does not contain any personal information and is used to de-duplicate reports and maintain accuracy in statistics. This token is deleted when the feature is disabled and a new token is regenerated when the feature is enabled again.

~~By default, the usage statistics do not include any personal information. However, if you're~~

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

that [no information can be inferred about any particular user's activity](#). This data collection mechanism is summarized on the [Google research blog](#), and full technical details have been published in a [technical report](#) and presented at the 2014 ACM Computer and Communications Security conference.

Chrome will also anonymously report to Google if requests to websites operated by Google fail or succeed in order to detect and fix problems quickly.

If you have also turned on “Make searches and browsing better (Sends URLs of pages you visit to Google)” in the “Sync and Google services” section of Chrome’s settings, Chrome usage statistics include information about the web pages you visit and your usage of them. The information will also include the URLs and statistics related to downloaded files. If you sync [extensions](#), these statistics will also include information about the extensions that have been installed from Chrome Web Store. The URLs and statistics are sent along with a unique device identifier that can be reset by turning off “Make searches and browsing better” in the “Sync and Google services” section of Chrome’s settings or by turning off usage statistics and crash reports. The usage statistics are not tied to your Google account. Google only stores usage statistics associated with published extensions, and URLs that are known by Google’s web crawlers. We use this information to improve our products and services, for example, by identifying web pages which load slowly; this gives us insight into how to best improve overall Chrome performance. We also make some statistics available externally, through efforts like the [Chrome User Experience Report](#). Externally published reports are conducted in highly aggregated manner to not reveal individual user's identity.

On iOS, if you are syncing your browsing history without a sync passphrase, Chrome reports usage for certain URLs that other Google apps could open. For example, when you tap on an email address, Chrome presents a dialog that allows you to choose between opening with

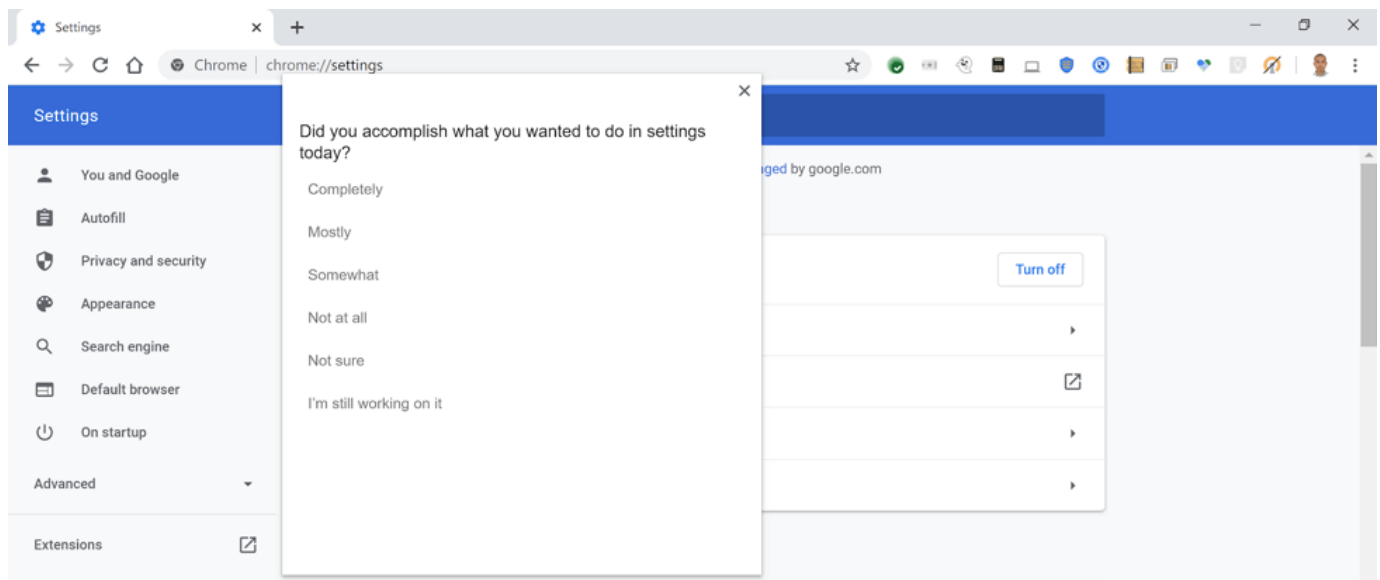
Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Google Surveys in Chrome

In Chrome on Android and Desktop, when you have "send usage statistics" enabled, you may be randomly selected to participate in surveys to evaluate consumer satisfaction with Chrome features. If you are selected, Chrome requests a survey from Google for you. If a survey is available, Chrome then asks you to answer the survey and submit responses to Google.

The survey also records basic metrics about your actions, such as time spent looking at the survey and elements that the user clicked. These metrics are sent to Google even if you do not fully complete the survey.

Google uses strategies to ensure that surveys are spread evenly across users and not repeatedly served to a single user. On Android, Chrome stores a randomly generated unique token on the device. On Desktop, Chrome uses a cookie to connect with the server. This token or cookie is used solely for the survey requests and does not contain any personal information. If you disable sending usage statistics, the token or cookie will be cleared.



Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

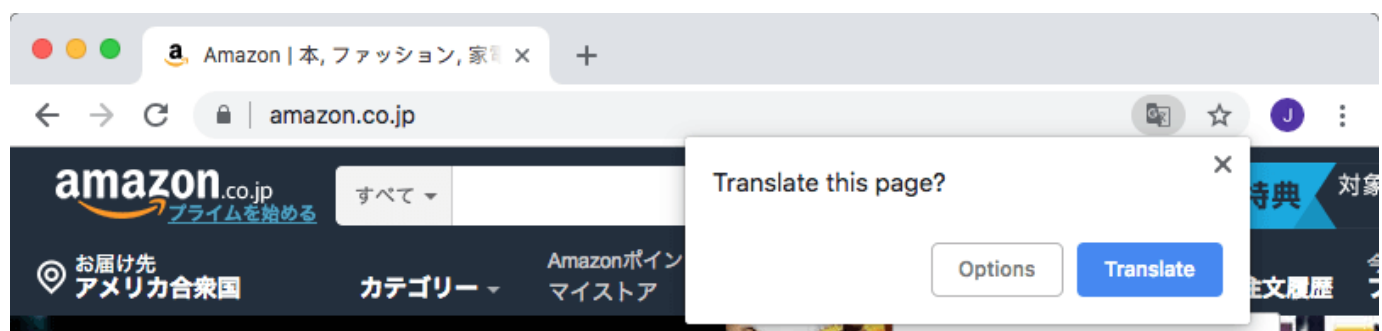
the browser to Google's servers, allowing you to apply the same spell-checking technology that's used by Google products like Docs. If this feature is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Google returns a list of suggested spellings that are displayed in the context menu. Cookies are not sent along with these requests. Requests are logged temporarily and anonymously for debugging and quality improvement purposes.

This feature is disabled by default; to turn it on, click "Ask Google for suggestions" in the context menu that appears when you right-click on a misspelled word. You can also turn this feature on or off with the "Enhanced spell check" checkbox in the "Sync and Google services" section of Chrome settings. When the feature is turned off, spelling suggestions are generated locally without sending data to Google's servers.

Mobile versions of Chrome rely on the operating system to provide spell-checking.

Translate

Google Chrome's built-in translation feature helps you read more of the Web, regardless of the language of the web page. The feature is enabled by default.



Translation [can be disabled at any time](#) in Chrome's settings.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Results Page.

If you do choose to translate a web page, the text of that page is sent to [Google Translate](#) for translation. Your cookies are not sent along with that request and the request is sent over SSL. This communication with Google's translation service is covered by the [Google privacy policy](#).

If you've chosen to sync your Chrome history, statistics about the languages of pages you visit and about your interactions with the translation feature will be sent to Google to improve Chrome's understanding of the languages you speak and when Chrome should offer to translate text for you.

Image Descriptions for screen reader users

Chrome can provide automatic descriptions for users who are visually impaired by sending the contents of images on pages you visit to Google's servers. This feature is only enabled when Chrome detects that the user has a screen reader running and if the user explicitly enables it in the page context menu. Cookies are not sent along with these requests. Chrome fetches the list of supported languages from Google's servers and then requests descriptions in the most appropriate language given the current web page and the user's language preferences. Requests are not logged.

Sign In to Chrome and sync

You have the option to use the Chrome browser while signed in to your Google Account, with or without [sync](#) enabled.

On desktop versions of Chrome, signing into or out of any Google web service, like google.com, signs you into or out of Chrome. On Chrome on Android, when you sign into any Google web service, Chrome may offer you to sign in with the accounts that are already signed in on the

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#).

When you're signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more. In advanced sync settings, you can choose which types of data to synchronize with this device. By default, all syncable data types are enabled. You can turn sync on or off in the "You and Google" section of Chrome settings.

If you have turned on sync and signed out of the account you are syncing to, sync will pause sending all syncable data to Google until you sign back in with the same account. Some sync data types (such as bookmarks and passwords) that are saved locally while sync is paused will automatically be synced to your account after you sign back in with the same account.

On mobile versions of Chrome, you can turn sync on or off in Chrome settings. This can be done for any account that has already been added to the mobile device without authenticating again.

On both desktop and mobile, signing into Chrome keeps you signed into Google web services until you sign out of Chrome. On mobile, signing into Chrome will keep you signed in with all Google Accounts that have been added to the device. On desktop, it will keep you signed in with all Google Accounts that you added from a Google web service, unless you have set "Clear cookies and site data when you quit Chrome" in your [cookie settings](#).

On Android and desktop, Chrome signals to Google web services that you are signed into Chrome by attaching an X-Chrome-Connected header to any HTTPS requests to Google-owned domains. On iOS, the CHROME_CONNECTED cookie is used instead. On Android, Chrome sends

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

data be deleted when you disconnect your account.

Users can share phone numbers and text between their devices (mobile or desktop) when they are signed-in to Chrome. The transferred data is encrypted during transit and Google cannot read or store the content. To let users select the device to share with, Chrome collects the following information about devices on which a user is signed-in and stores that in the user's Google account: device manufacturer, model number, Chrome version, OS, and device type.

Google uses your personal synchronized data to provide you a consistent browsing experience across your devices, and to customize features in Chrome. You can manage your synchronized history by going to [chrome://history](#) in your Chrome browser. If “Include history from Chrome and other apps in your Web & App Activity” is checked on the [Web & App Activity](#) controls page, Google also uses your synchronized browsing data to provide personalized Google products and services to you. You can change your preference any time, and manage individual [activities associated with your Google account](#).

The paragraph above describes the use of your personal browsing history. Google also uses aggregated and anonymized synchronized browsing data to improve other Google products and services. For example, we use this information to improve Google Search by helping to detect mobile friendly pages, pages which have stopped serving content, and downloads of malware.

For sync users, Google may collect additional information derived from Chrome history for the [Federated Learning of Cohorts](#) (FLoC) experiment. FLoC is one of the open standards proposed as part of the [Privacy Sandbox](#), an initiative to make the web more private and secure for users while also supporting publishers. Chrome's implementation of FLoC assigns each user to an interest cohort - a cluster representing a large group of users who share similar browsing habits - and periodically updates this assignment by similarity-hashing recently visited URLs from

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

If you would like to use Google's cloud to store and sync your Chrome data without allowing any personalized and aggregated use by Google as described in the previous paragraphs, you can choose to encrypt all of your synced data with a [sync passphrase](#). If you choose this option, it's important to note that Google won't have access to the sync passphrase you set; we won't be able to help you recover data if you forget the passphrase. Regardless of how you choose to encrypt your data, all data is always sent over secure SSL connections to Google's servers.

Google will store the metadata about the days on which sync was running to improve other Google products and services.

Chrome may help you sign in with credentials you've saved in Android apps on websites that are associated with the respective apps. Likewise, credentials you've saved for websites can be used to help you sign into related Android apps. You can view the credentials you've saved in Chrome and Android by visiting passwords.google.com in any browser. If you've saved credentials for Android applications, Chrome periodically sends a cookieless request to Google to get an updated list of websites that are associated with those applications. To stop websites and Android apps from automatically signing in using credentials you previously saved, you can turn off Auto Sign-In on passwords.google.com or in Chrome settings under "Autofill > Passwords". For more details see [this article](#).

To make the history page easier to use, Chrome displays favicons of visited URLs. For Chrome browsing history from your other devices, these favicons are fetched from Google servers via cookieless requests that only contain the given URL and device display DPI. Favicons are not fetched for users with sync passphrase.

On the iOS version of Chrome, if you sync your browsing history without a sync passphrase and your browser's usage statistics and crash reports setting is also enabled, your usage statistics

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

[Google Dashboard](#). That page also allows you to stop synchronization completely and delete all sync data from Google's servers.

Autofill and Password Management

Google Chrome has a [form autofill feature](#) that helps you fill out forms on the web more quickly. Autofill is enabled by default, but it can be turned off at any time in Chrome's settings.

If Autofill is enabled and you encounter a web page containing a form, Chrome sends some information about that form to Google. This information includes the basic structure of the form, a hash of the web page's hostname as well as form identifiers (such as field names); randomized representation of the form identifiers, and if you have turned on the "Make searches and browsing better (Sends URLs of pages you visit to Google)" setting, also a randomized representation of the web page's URL. In response, Chrome receives a prediction of each field's data type (for example, "field X is a phone number, and field Y is a country"). This information helps Chrome match up your locally stored Autofill data with the fields of the form.

If Autofill is enabled when you *submit* a form, Chrome sends Google some information about the form along with the types of data you submitted. This information includes a hash of the web page's hostname, as well as form identifiers (such as field names), the basic structure of the form, and the observed data types for the fields (i.e., field X was a phone number, field Y was a country). The values you entered into the form are not sent to Google. This information helps Chrome improve the quality of its form-filling over time.

You can manage your Autofill entries via [Chrome's settings](#), and you can edit or delete saved information at any time. Chrome will never store full credit card information (card number, cardholder name, and expiration date) without explicit confirmation. In order to prevent offering to save cards you have shown disinterest in saving, Chrome stores the last four digits of

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

or by automatically signing you in. You can manage and delete your saved credentials in the “Forms and passwords” section of Chrome’s settings. If you enable [password management](#), the same kind of data about forms as described above is sent to Google to interpret password forms correctly. To enable Chrome to offer password generation that meets site-specific requirements, Chrome uploads a randomized vote on a specific password characteristic to the server once a user-created password is stored. If stored credentials are used for the first time in a username field which was already filled differently by the website itself, Chrome also transmits a short one-byte hash of the prefilled value. This allows Google to classify if the website uses a static placeholder in the username field which can be safely overwritten without deleting valuable user-specific data. Google cannot reconstruct the value from this hash.

When you’re signed in to Chrome with your Google Account on desktop, Chrome may offer you to use credentials you’ve saved to your account, to generate a strong password, or to save credentials to your Google Account. To access credentials in your Google Account, Chrome may ask you to re-authenticate to your Google Account. Credentials from your Google Account will be available on the device while you’re signed in, even when you are offline. If sync isn’t enabled, when you sign out of Chrome, all credentials stored in your Google Account are removed from Chrome on the device. While signed in to Chrome, you can choose to store a credential after you have signed into a site to your Google Account or locally to the device. Locally-saved credentials are not deleted when you sign out of Chrome. After you have used a locally-saved credential to sign into a site, Chrome may also offer you to move the locally stored credentials to your account.

When you sign in to a site, Chrome may give you a [warning](#) if the username/password have been exposed as a result of a data breach on some website or app. The feature is available on all platforms but only to the users signed in with a Google account. On Android the feature is only available if sync is also enabled, due to the way the accounts are managed by the OS. Being

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

the database. The feature can be disabled in settings under Sync and Google services. On desktop and Android versions of Chrome, this feature is not available if Safe Browsing is turned off.

Using the same secure method described above, you can check all the saved passwords against the public data breaches in the “Passwords” section of Chrome’s settings. Once you’ve run a password check, Chrome will show a list of breached passwords. If a password in this list is outdated, you can manually edit it to store the current version. If you choose to edit, the new username/password pair will be checked automatically but only if the feature described above is not disabled.

Also, if you choose, you can bring your Autofill data with you to all your Chrome-enabled devices by [syncing it](#) as part of your browser settings (see the “Sign In to Chrome” section of this document). If you choose to sync Autofill information, field values are sent as described in “Sign In to Chrome”; otherwise, field values are not sent.

If you enable Chrome’s credential provider extension in iOS Autofill passwords settings, Chrome will be able to autofill the passwords currently saved in Chrome into other apps on your device, such as Safari. The extension does not store Chrome passwords. If the device's keychain or the iCloud keychain are enabled as a credential provider, then the extension will prompt you to save the recently used password in the keychain.

Payments

When you’re signed into Chrome with your Google Account, Chrome may offer to save payment cards and related billing addresses into payment data under the same Google Account, and include cards from your account among the autofill suggestions on payment web forms. If you're not signed in, Chrome offers to save your credit cards locally. If the card is not stored locally, you

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

prompted for your CVV code or device authentication each time you use the card. You can [opt out of using device authentication](#) in the Payment methods section of Chrome settings. If you use a card from Google Payments, Chrome will collect information about your computer and share it with Google Payments to prevent fraudulent use of your card. If you use device authentication to confirm cards from Google Payments, an identifier scoped to a device and signed-in session will be used to ensure that the device and account autofilling the card should have access to it.

To delete credit card information saved in Chrome, follow the “Add and edit credit cards” steps in [the Autofill article](#). When you delete a credit card that's also saved in your Google Payments account, you will be redirected to Google Payments to complete the deletion. After your card has been deleted from your Google Payments account, Chrome will automatically remove that card from your Autofill suggestions.

To save a card locally on the device only, while still being signed in to Chrome with a Google Account, you can add a card from the “Add” button in the “Payment methods” section in Chrome settings. If you would like to sign into Google web services, like google.com, without Chrome asking whether you want to save your info to your Google Account, you can [turn off Chrome sign-in](#). If you have sync turned on, you can disable syncing payment methods and addresses to Google Pay under “Sync” in Chrome settings. You can also turn the Payments Autofill feature off altogether in [settings](#).

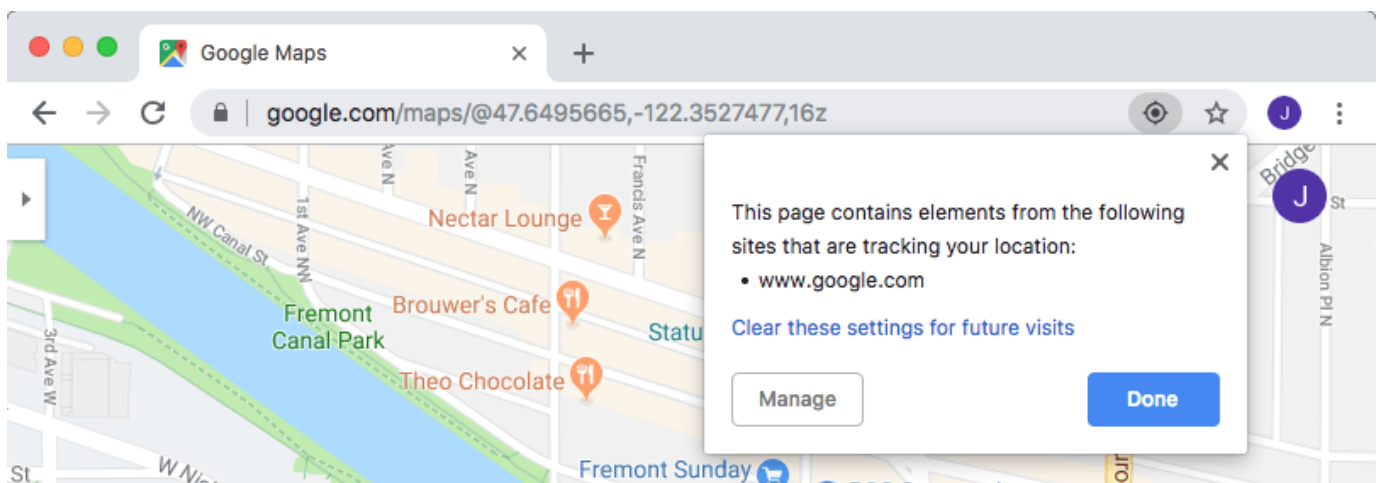
Chrome also supports the [PaymentRequest API](#) by allowing you to pay for purchases with credit cards from Autofill, Google Payments, and other payment apps already installed on your device. Google Payments and other payment apps are only available on Android devices.

PaymentRequest allows the merchant to request the following information: full name, shipping address, billing address, phone number, email, credit card number, credit card expiration, CVV,

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

By default, Chrome will request your permission when a web page asks for your location information, and does not send any location information to the web page unless you explicitly consent.

Furthermore, whenever you are on a web page which is using your location information, Chrome will display a location icon on the right side of the omnibox. You can click on this icon in order to find out more information or manage location settings.



In [Chrome's settings](#), by clicking "Site Settings" and scrolling to the "Location" section, you can choose to allow all sites to receive your location information, have Chrome ask you every time (the default), or block all sites from receiving your location information. You can also configure exceptions for specific web sites.

In the Android version of Chrome, your default search engine automatically receives your location when you conduct a search. On the iOS version of Chrome, by default your location is sent to Google if you conduct a search from the omnibox. Read more about how your default search engine handles geolocation and how to manage your settings in the [Omnibox](#) section of

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

and improve the overall quality of Google Chrome and Google Location Services.

For further reading on the privacy and user interface implications of the Geolocation API (as well as other HTML5 APIs), see ["Practical Privacy Concerns in a Real World Browser"](#) written by two Google Chrome team members.

Speech to text

Chrome supports the [Web Speech API](#), a mechanism for converting speech to text on a web page. It uses Google's servers to perform the conversion. Using the feature sends an audio recording to Google (audio data is not sent directly to the page itself), along with the domain of the website using the API, your default browser language and the language settings of the website. Cookies are not sent along with these requests.

Google Assistant on ChromeOS devices

The Google Assistant is integrated into some models of ChromeOS devices. If you opt in to the feature, ChromeOS listens for you to say "Ok Google" and sends the audio of the next thing you say, plus a few seconds before, to Google. Detection of the phrase "Ok Google" is performed locally on your computer, and the audio is only sent to Google after it detects "Ok Google". You can enable or disable this feature in Google Assistant Settings.

Enabling this feature in Chrome Settings will cause Chrome to listen whenever the screen is unlocked. On ChromeOS devices with a local audio processor, the device also listens when the device is asleep. On these devices, The Google Assistant feature only works if [Voice & Audio Activity](#) is enabled for your Google account. Chrome will prompt you to enable [Voice & Audio Activity](#) for the associated Google account if it is disabled.

Once the audio has been converted to text, a search with that text is submitted to Google. If you

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Google Assistant on Android devices

You can quickly complete tasks on the web using the Google Assistant in Chrome on certain Android devices . If you opt-in to this feature, you can speak to the Google Assistant and ask it to search websites. It also can fill out forms on your behalf, or speed up the checkout experience.

For example, if you issue a command to the Google Assistant e.g. “search Wikipedia for Henry VIII”, the Google Assistant in Chrome will respond by opening Chrome to Wikipedia, sending the query as a text string to Google Assistant in Chrome, and searching for “Henry VIII” on the Wikipedia page.

As another example, if you ask the Google Assistant to help you purchase tickets for an upcoming movie, then the address of the website you are viewing, your credit card information, and your email address will be shared with Google to complete the transaction and make it possible for you to receive the purchase receipt and movie ticket.

If you opt-in to this feature, the Google Assistant in Chrome will send data to Google in order to complete the command you issued. When the command is issued, the Google Assistant in Chrome shares back to Google the website’s URL to validate that the webpage is allowed to be automated by Google Assistant in Chrome and to receive the instructions on how to complete the task (e.g. on how to fill out a form).

At the time the command you issued is executed, additional information can be shared. Depending on the command you issued, the information shared with Google can include the address of the website you are viewing, your email address, your name, your delivery and billing address, your credit card information, and possibly the username you use to log into the website. This information is not stored by Google — rather, this information is passed on to the third party

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Some Google Assistant features are not available on Incognito tabs. You can turn off the ability to use the Google Assistant in Chrome on your Android device by toggling the “Google Assistant for Chrome” option in Chrome’s settings.

Google Cloud Print

The [Google Cloud Print](#) feature allows you to print documents from your browser over the Internet. You do not need a direct connection between the machine that executes Chrome and your printer.

If you choose to print a web page via Cloud Print, Chrome will generate a PDF of this website and upload it over an encrypted network connection to Google’s servers. If you choose to print other kinds of documents, they may be uploaded as raw documents to Google’s servers.

A print job will be downloaded by either a Chrome browser (“Connector”) or a Cloud Print capable printer that you selected when printing the website. In some cases the print job must be submitted to a third-party service to print (HP’s ePrint, for example).

The print job is deleted from Google’s servers when any of three criteria is met:

- You delete the print job
- The job has been printed and marked as printed by the printer/connector
- The job has been queued on Google’s servers for 30 days

You can manage your printers and print jobs on the [Google Cloud Print website](#).

SSL certificate reporting

Chrome stores locally a list of expected SSL certificate information for a variety of high-value

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

You can enable this feature by opting in to report data relevant to security, as described in the [Safe Browsing section](#). While you are opted in, two kinds of reports may be sent to Google's security team. Each time you see an SSL error page, a report will be sent containing the SSL certificate chain, the server's hostname, the local time, and relevant details about the validation error and SSL error page type. Additionally, each time a mismatch between different certificate verifiers is detected, a report will be sent containing the certificate chain and the verification result.

Because Chrome sends these reports for all certificate chains, even those that chain to a private root of trust, these chains can contain personally identifiable information. You can opt out anytime by unchecking the box "Help Improve Chrome security" in "Privacy and security > Security".

The SSL certificate reporting feature is not available on Chrome iOS.

Installed Applications and Extensions

Users can install external apps and extensions for the desktop versions of Chrome to add features to or customize their Chrome browsers. Installing an application or extension from the Chrome Web Store directly or via an [inline installation](#) flow on a third-party site involves a request to the Chrome Web Store for details about the application. This request includes cookies, and if you're logged into Google when you install an application, that installation is recorded as part of your Google account. The store uses this information to recommend applications to you in the future, and in aggregate to evaluate application popularity and usage. As noted above, applications and extensions are updated via Google Update.

As they're more deeply integrated into Chrome, applications and extensions that you choose to

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

the time to read and evaluate this warning before proceeding with the installation. Note also that interactions with and data collected by these third-party applications and extensions are governed by their own privacy policies, not Google's privacy policy.

Push messaging

Your device may receive push messages from the backend servers of apps and extensions installed in Chrome, websites that you grant the “notification” permission to, and your default search engine. Disabling push messages from your default search engine is done in the same way as disabling push messages from any site, by visiting the “Notifications” section of “Site settings”.

Push message data is sent over a secure channel from the developer through Google’s infrastructure to Chrome on your device, which can wake up apps, extensions, and websites (including your default search engine) to deliver the message. The developer may end-to-end encrypt the message data, or may send it in a form such that Google servers process it as plain text. Google servers retain up to 4 weeks’ worth of messages to ensure delivery to users even if their devices are offline at the time of the initial pushing.

If the notification permission is set to “granted” for any website (including the default search engine), or you have an app or extension installed that uses push messaging, then Chrome provides the app’s, extension’s, or website’s server with one or more registration tokens that can be used to send messages to the entity (app, extension, or website). Websites you visit in Incognito mode are not allowed to send you push messages and therefore cannot get a registration token.

When you uninstall an app or extension, revoke the notification permission for a website, or clear cookies for a permitted website, its registration token is revoked and will not be reused, even if

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

encryption is designed so that two registration tokens for the same device ID cannot be correlated. On desktop versions of Chrome, the device ID is reset when the Chrome profile is removed, or when neither Chrome Sync nor any of the entities requires it for push messaging. On Android, the lifetime of the device ID is governed by the operating system and is independent of Chrome. Any messages routed to registration tokens containing a revoked device ID will not be delivered.

Chrome custom tabs

On Android devices, an app developer may use a Custom Tab to show web content when you click on a URL from their app. A Custom Tab may look different from a regular Chrome tab, for example it may have app-specified visual style, and the absence of an editable URL bar. Despite the different visual style a Custom Tab may have, the data sent and received in the Custom Tab, such as cookies, saved passwords and browsing history function the same way they do in a normal Chrome tab. The Custom Tab is an app-customized view using the same underlying user profile.

With Chrome Custom Tabs, an Android app developer may also specify custom actions in the Chrome toolbar and overflow menu that are relevant to their app, for example, "share", "save page", "copy URL". If you tap on such a button, the address of the current website is shared with the application.

An application can request Chrome to pre-render a given URL in the background. This allows Chrome to show you a pre-loaded site instantly when you open it from the app. At the same time it allows an application to set cookies in your browser in the background. To disable pre-rendering, you can uncheck "Preload pages for faster browsing and searching" in the "Privacy and security > Cookies" section of Chrome's settings.

Continue where you left off

If you have selected the option to "Continue where you left off" in settings on desktop versions of Chrome, when you open Chrome, it attempts to bring you right back to the way things were when the browser was closed. Chrome reloads the tabs you had open and persists session information to get you up and running as quickly as possible. This feature effectively extends a browsing session across restarts. In this mode, session cookies are no longer deleted when the browser closes; instead, they remain available on restart to keep you logged into your favorite sites.

On desktop versions of Chrome, this feature can be enabled or disabled in Chrome settings. On ChromeOS, it is enabled by default.

On MacOS, when you restart your device, a checkbox in the OS confirmation dialog asks you whether you want to re-open applications and windows after restart. If you check this box, Chrome restores tabs and windows, as well as the session cookies, even if you have disabled "Continue where you left off" on Chrome.

On mobile versions of Chrome, this feature is always enabled without a setting.

Chrome Variations

Chrome is constantly evolving to better meet the needs of users and the web. To ensure new features are providing the best experience and working correctly, they may be enabled for a subset of users before they are fully launched. For example, if we improve how page loading works in Chrome, we may try it out for 1%% of users to ensure that it doesn't crash or run slower before launching to everyone. This is done through a system called "Chrome Variations" - also known as "field trials"

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Chrome installations that have [usage statistics reporting enabled](#).

Other factors may additionally inform the variations assigned to a Chrome installation, such as country (determined by your IP address), operating system, Chrome version and other parameters.

Usage statistics and crash reports are tagged with all variations a client participates in, including both low entropy and high entropy variations. These reports, which also contain a pseudonymous client identifier, can be disabled in Chrome settings.

Additionally, a subset of low entropy variations are included in network requests sent to Google. The combined state of these variations is non-identifying, since it is based on a 13-bit low entropy value (see above). These are transmitted using the "X-Client-Data" HTTP header, which contains a list of active variations. On Android, this header may include a limited set of external server-side experiments, which may affect the Chrome installation. This header is used to evaluate the effect on Google servers - for example, a networking change may affect YouTube video load speed or an Omnibox ranking update may result in more helpful Google Search results.

On Android Chrome, in certain cases these low entropy variations may also be sent to Google apps when cross-app communication occurs to support a Chrome feature; for example, when searching with [Google Lens](#). This information is used to better understand how Chrome experiments affect that Google feature: for example, Chrome memory usage change could affect how long it takes an action in the Google app to complete.

You can reset the variations used by your Chrome installation by starting it with the "--reset-variation-state" command line flag.

Do Not Track

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

The effect of Do Not Track depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example, to improve security; to provide content, services, ads and recommendations on their websites; and to generate reporting statistics.

Chrome on iOS now uses WKWebView to provide a more stable and faster browser. As a result of this move, the Do Not Track preference is no longer available due to iOS constraints. If Apple makes changes to allow this feature, Chrome will make Do Not Track available again in iOS.

Plugins

Chrome ships with an Adobe Flash Player implementation that is based on the Pepper API. Flash and other Pepper-based plugins may ask you for “Access to your computer”. If you grant this permission, the plugin is granted unsandboxed access. This allows content providers to offer you access to DRM protected content like videos or music but may have security and privacy implications, so consider carefully whether you trust a plugin or website with this privilege.

Media licenses

Some websites encrypt media to protect against unauthorized access and copying. When users play media from these sites, they typically log into the site, which authenticates the user, and then digital rights management negotiates a key exchange for the decryption and playback of the media.

For HTML5 sites, this key exchange is done using the Encrypted Media Extensions API. The implementation of that API is tightly coupled with the browser to protect user privacy and security through Content Decryption Modules (CDM), which are provided by digital rights

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

request is typically sent to a license server managed by either the content website or Google. Neither the license request, the proof, nor the request ID include any personally identifying information. After being sent, the license request is not stored locally on the user's device.

As part of the license request, Chrome also generates a unique session ID which does not contain personally identifying information. This session ID is sent to the license server, and when the server returns a license the session ID is used to decrypt the media. The session ID may be stored locally even after the site has been closed. The license may also be stored locally for offline consumption of protected content. Session ID and licenses may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected.

When returning a license, the site license server may include a client ID, generated by the site. This client ID is unique to the user and the site, it is not shared between sites. If provided, the client ID is stored locally and included by Chrome in subsequent license requests to that site. The client ID may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected.

On some platforms, the website may additionally request verification that the device is eligible to play specific types of protected content. On ChromeOS, this is known as [Verified Access](#). In this case, Google creates a certificate using a unique hardware identifier for the device. This hardware ID identifies the device, but does not identify the user. If the user agrees, Google receives the hardware ID and generates a certificate verifying the device for the requested site. The certificate does not include the hardware ID or any other information that could permanently identify the device. Certificates are stored locally similar to other cached browsing data, and may be cleared by the user in Chrome using [Clear Browsing Data](#) with "Cookies and other site data" selected. On Android, this is called [Provisioning](#). See "[MediaDrm Provisioning](#)" for more details.

from a unique file on your disk. This identifier can be reset by reinstalling your operating system.

MediaDrm provisioning

Chrome on Android uses [Android MediaDrm](#) to play protected content. As on ChromeOS, the website may request verification that the device is eligible to do so. This is achieved by MediaDrm provisioning. A provisioning request is sent to Google, which generates a certificate that will be stored on the device and sent to the site whenever you play protected content. The information in the provisioning request and in the certificate vary depending on the Android version. In all cases, the information can be used to identify the device, but never the user.

On Android K and L, the device only needs to be provisioned once and the certificate is shared by all applications running on the device. The request contains a hardware ID, and the certificate contains a stable device ID, both of which could be used to permanently identify the device.

On Android M or later, MediaDrm supports per-origin provisioning. Chrome randomly generates an origin ID for each website to be provisioned. Even though the request still contains a hardware ID, the certificate is different for each website, so that different websites cannot cross-reference the same device.

On Android O or later on some devices, provisioning can be scoped to a single application. The request will contain a hardware ID, but the certificate will be different for each application, in addition to each site, so different applications cannot cross-reference the same device.

Provisioning can be controlled by the “Protected media” permission in the “Site settings” menu. On Android versions K and L, Chrome will always ask you to grant this permission before provisioning starts. On later versions of Android, this permission is granted by default. You can clear the provisioned certificates anytime using the “Cookies and other site data” option in the

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

have already been provisioned by other applications.

On Android versions with per-origin provisioning, Chrome pre-provisions itself once the user attempts to play protected content. As the provisioning for the first playback already involved sending a stable hardware ID to Google, the subsequent pre-provisioning of additional origin IDs introduces no new privacy implications. If provisioning fails and there is no pre-provisioned origin ID, Chrome may ask for permission to further fallback to per-device provisioning.

On devices with per-application provisioning, Chrome pre-provisions itself automatically on startup.

Cloud policy

When you sign into a ChromeOS device, Chrome on Android, or a desktop Chrome profile with an account associated with a Google Apps domain, or if your desktop browser is enrolled in Chrome Browser Cloud Management, Chrome checks whether the domain has configured enterprise policies. If so, the ChromeOS user session, Chrome profile, or enrolled Chrome Browser is assigned a unique ID, and registered as belonging to that Google Apps domain. Any configured policies are applied. To revoke the registration, remove the ChromeOS user, sign out of Chrome on Android, remove the desktop profile, or [remove the enrollment token and device token](#) for Chrome Browser Cloud Management.

Additionally, ChromeOS devices can be enrolled to a Google Apps domain by a domain admin. This will enforce enterprise policies for the entire device, such as providing shared network configurations and restricting access to developer mode. When a ChromeOS device is enrolled to a domain, then a unique device ID is registered to the device. In order to revoke the registration, the admin will need to wipe the entire ChromeOS device.

Lite Mode

If you enable Lite Mode (previously known as “Data Saver”), Chrome may send your traffic through Google's optimizing servers to reduce the amount of data downloaded and speed up your page loads.

Chrome will share the URLs you visit with Google, as well as usage and performance statistics for those sites so Chrome can better optimize them. Cookies for sites you visit are not shared with Google. Logs are not associated with your Google Account, and all log entries are removed within 14 days. Pages loaded in Incognito will not use the optimizing servers and usage and performance statistics will not be reported.

Image Compression

To save Lite Mode users data, image requests may be sent to a Google image optimization server which will fetch the image from the origin and return a compressed version to Chrome. To avoid optimizing private images, Chrome first asks Google for a list of image URLs known to be on the page according to a crawl of the site from a Google data center. Only images on that list will be sent to the optimization server. Image URLs on the page that were not seen during the Google crawl will not be optimized, and no information about those URLs will be sent to Google.

Using Chrome with a kid’s Google Account

Chrome for Android offers features to be used when signed in with a [kid's Google Account](#) and automatically signs in a kid's account if they've signed into the Android device. Chrome uses the [Sync feature](#) to sync settings configured by parents to the kid’s account. You can read about how Sync data is used in the [Sign in](#) section of this Whitepaper.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

deleting browsing history from within Chrome. Browsing history can still be removed in the [Chrome section of the Google Dashboard](#).

By default, first party cookie blocking is disabled when Chrome is signed in with a kid's account. Parents can go to chrome.google.com/manage/family to allow their kids to block first party cookies. However, blocking cookies signs kids out of Google web products such as Google Search or YouTube and therefore prevents these products from providing any features designed for kids' Google Accounts.

When Chrome is used with a kid's Google Account, information about the kid's requests to access blocked content is sent to Google and made visible to the kid's parent(s) on chrome.google.com/manage/family and in the [Google Family Link app](#). If the kid's browsing mode is set to "Try to block mature sites", Chrome will send a request to the Google [SafeSearch service](#) for each navigation in order to block access to sites that have been classified as containing mature content.

Incognito and Guest Mode

Incognito mode in Chrome is a temporary browsing mode. It ensures that you don't leave browsing history and cookies on your computer. **The browsing history and cookies are deleted only once you have closed the last incognito window. Incognito mode cannot make you invisible on the internet.** Websites that you navigate to may record your visits. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Browsing as a Guest in Chrome allows you to use somebody else's computer without modifying their profile. For example, no bookmarks or passwords get stored on their computer. Note that Guest mode does not protect you for example, if the computer you are using is infected by a keylogger that records what you type.

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

more information is available at [Apple Support](#), [Apple Developers](#), and in the [Apple iOS Security Guide](#). Chrome support for this feature can be disabled in Chrome settings.

Security Key

A FIDO U2F Security Key provides a non-phishable credential which can be used to authenticate a user. This mitigates the risk of various kinds of man-in-the-middle attacks in which websites try to steal your password and use it later.

To prevent abuse, a website is required to be delivered over a secure connection (HTTPS), and to register the security key before it can be used for identification. Once a website is registered with a specific security key, that security key will provide a persistent identifier, regardless of which computer it is plugged into, or whether you're in incognito or guest mode, but you must physically interact with the security key to give a website access to an identifier (by, for example, touching it, or plugging it in).

Physical Web

The Physical Web lets you see a list of URLs being broadcast by objects in the environment around you. Google Chrome looks for Physical Web devices with Bluetooth Low Energy beacons that are broadcasting URLs using the Eddystone protocol. Bluetooth signals can be received from 90 feet away or more, depending on signal strength and the user's environment (although the range is often much shorter, due to obstacles and signal noise). If the Physical Web feature is enabled, Chrome sends detected URLs to Google's Physical Web Service (PWS) via a cookieless HTTPS request. For each URL, the PWS obtains the title of the web page, filters out unsafe results, and returns a ranking based on non-personalized signals about the quality and relevance of the web page.

The Physical Web feature is available on Chrome on iOS and Android. Users will need to turn on

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

Once a user enables the feature, Chrome scans for nearby devices for a few seconds each time the user unlocks the mobile device in use and sends them to the PWS in order to obtain more information about the beacon. The user receives a silent notification when Chrome finds a nearby URL.

On iOS devices, users can [enable](#) (or disable) the feature in the Privacy settings or by adding the [Chrome widget to their Today view](#) in the notification center. Additionally, the feature is automatically enabled for users who have location enabled on their device, granted Chrome the location permission, and have granted Google the geolocation permission. Chrome scans for nearby devices whenever it is open in the foreground. When Chrome finds nearby URLs, users will see them as omnibox suggestions. Additionally, Chrome scans for nearby devices for a few seconds when the Today widget is displayed in the notification center.

Bluetooth

Google Chrome supports the [Web Bluetooth API](#), which provides websites with access to nearby [Bluetooth Low Energy devices](#) with your consent.

Chrome does not let any page communicate with a device unless you explicitly consent. When a web page asks to pair with a device, Chrome will ask you to choose which device the web page should access, if any. Selecting a device for one page does not give other pages access to the device you have chosen, and does not allow that page to access other devices. Currently, permission for a page to communicate with a device is usually revoked when the page is reloaded, and is always revoked when Chrome is restarted.

Chrome data that Android sends to Google

The data collection and usage described in this section is handled by Android and governed by

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

previously set up device. If you do so, Android may restore backed up Chrome preferences when Chrome is first installed. The new device only copies the preferences if automatic restore is enabled (see “Restore your data and settings” in [the same article](#)), Chrome was signed into an account when the backup was made, and the new Android device is signed into that same account.

Chrome’s backup data for a particular device may also be restored if you uninstall and then later re-install Chrome on that device. This will only happen if automatic restore is enabled and the device is signed into the account that Chrome was signed into when the backup was made.

Integration with Digital Wellbeing

If you opt-in to see sites you have visited and set site timers in the Digital Wellbeing app on Android, Chrome will report which websites you’ve visited and the length of time spent in each of them to the app. Sites visited in incognito mode will not be reported to the Digital Wellbeing app.

To continually improve the experience of Digital Wellbeing, the app will share with Google the websites that you set a timer on and how long you have visited them.

You can opt out of this feature in the Digital Wellbeing app or in Chrome’s privacy settings anytime.

Follow us



Chrome Family



Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).



Dev and Partners



Stay Connected



Google

[Privacy and Terms](#)

[About Google](#)

[Google Products](#)

 Help

Google uses cookies to deliver its services, to personalize ads, and to analyze traffic. You can adjust your privacy controls anytime in your [Google settings](#) or [read our cookie policy](#).

EXHIBIT 142

**4/29/21 David
Monsees Deposition
Transcript Excerpts**

**Redacted Version of
Document Sought to
be Sealed**

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, ELAINE CRESPO,)
HADIYAH JACKSON and CLAUDIA)
KINDLER, on behalf of all)
others similarly situated,)
Plaintiffs,)
vs.) Case No.
GOOGLE LLC,) 5:20-cv-5146-LHK
Defendant.)
_____)

VIRTUAL VIDEOCONFERENCE VIDEO-RECORDED
DEPOSITION OF DAVID MONSEES

Friday, April 9, 2021
Testifying from San Francisco, California

Reported By:
Hanna Kim, CLR, CSR No. 13083
Job No. 4530995

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, ELAINE CRESPO,)
HADIYAH JACKSON and CLAUDIA)
KINDLER, on behalf of all)
others similarly situated,)
Plaintiffs,)
vs.) Case No.
GOOGLE LLC,) 5:20-cv-5146-LHK
Defendant.)
_____)

Virtual videoconference video-recorded
deposition of DAVID MONSEES, taken on
behalf of the Plaintiffs, testifying from
San Francisco, California, on Friday,
April 9, 2021, before Hanna Kim, CLR, CSR
No. 13083.

REMOTE VIDEOCONFERENCE APPEARANCES OF COUNSEL:

For Plaintiffs:

BLEICHMAR FONTI & AULD LLP

BY: LESLEY WEAVER, ESQ.

BY: ANGELICA M. ORNELAS, ESQ.

555 12th Street, Suite 1600

Oakland, California 994607

415.445.4003

lweaver@bfalaw.com

aornelas@bfalaw.com

-and-

KAPLAN FOX & KILSHEIMER LLP

BY: DAVID A. STRAITE, ESQ.

850 Third Avenue

New York, New York 10022

212.687.1980

dstraite@kaplanfox.coma

REMOTE VIDEOCONFERENCE APPEARANCES (CONTINUED)

For Plaintiffs:

SIMMONS HANLY CONROY LLC

BY: JASON "JAY" BARNES, ESQ.

BY: AN TRUONG, ESQ.

112 Madison Avenue, 7th Floor

New York, New York 10016

212.784.6400

jaybarnes@simmonsfirm.com

atruong@simmonsfirm.com

For Defendant Google LLC:

QUINN EMANUEL URQUHART & SULLIVAN

BY: ANDREW H. SCHAPIRO, ESQ.

191 N. Wacker Drive, Suite 2700

Chicago, Illinois 60606

312.705.7400

andrewschapiro@quinnemanuel.com

-and-

BY: JOSEF ANSORGE, PH.D.

1300 I Street NW, Suite 900

Washington, D.C. 20005

202.538.8000

josefansorge@quinnemanuel.com

1 (Short recess taken.)

2 THE VIDEOGRAPHER: We are now back on the
3 record. The time is 10:46 a.m. Pacific Daylight
4 Time.

5 BY MS. WEAVER: 10:47:04

6 Q. You understand that you're still under
7 oath; correct?

8 A. I do.

9 Q. Okay. I want to return very quickly just
10 to Exhibit 3 and ask you to turn back to the first 10:47:13
11 page of it, in the drop-down.

12 A. Okay.

13 Q. I asked you about IP.

14 Do you see there's a drop-down that says
15 "IP"? 10:47:25

16 A. I do.

17 Q. And -- and I can't recall, did -- do you
18 know what IP is?

19 A. I -- I do not know what it stands for
20 here. 10:47:31

21 Q. Okay. What is an IP address?

22 A. An IP address is a ID generated by your
23 internet service provider that's used to connect
24 traffic on the internet, how devices and servers
25 work on the -- on the internet. 10:47:49

Page 83

1 Q. Okay. Is it possible that this refers to
2 IP address?

3 MR. SCHAPIRO: Objection. Calls for
4 speculation.

5 THE WITNESS: I was going to say, I would 10:48:00
6 have to speculate.

7 BY MS. WEAVER:

8 Q. Okay. Do you know who would know if this
9 refers to IP address?

10 A. I -- I do not know. 10:48:05

11 Q. You can't identify anybody who would know
12 whether or not this refers to IP address?

13 A. Not an individual that I know.

14 Q. Okay. Is there a team that would know?

15 A. I -- I'm not sure of a specific team that 10:48:15
16 would know either.

17 Q. Okay. And you recall earlier, you were --
18 you explained what a user agent -- do you -- is.

19 Do you recall that?

20 A. (Witness nods.) 10:48:31

21 Q. Do you mind repeating that for the record?

22 A. The -- or the reporter could read back,
23 but I -- I can try and --

24 Q. No, that's fine.

25 Can you define what a user agent is? 10:48:39

1 A. Yeah. The -- the user agent is the string
2 and information that any browser provides to
3 identify the type of browser. And some of the
4 examples of information that I gave that might be
5 included in the user agent is the browser type, 10:48:56
6 the browser version, and the operating system and
7 the operating system version for which that
8 browser is running on.

9 Q. And does the user agent also include IP
10 address? 10:49:10

11 A. I believe the IP address comes separately
12 in a request and is not part of the user agent.

13 Q. Okay. Great.

14 I am going to mark one more document to
15 just get some definitions in place before we look 10:49:22
16 at the Complaint.

17 MS. WEAVER: So we'll mark as Exhibit 4, a
18 document bearing Bates numbers GOOG-CALH '22 --
19 sorry -- '27774 through '781.

20 (Monsees Deposition Exhibit 4 was marked.) 10:49:51

21 MS. ORNELAS: Exhibit 4 has been
22 published.

23 BY MS. WEAVER:

24 Q. And, Mr. Monsees, please let me know when
25 you have the document. 10:49:58

1 A. Give me one moment.

2 Okay. I -- I have the document up.

3 Q. And have you seen Exhibit 4 before?

4 A. Yes, I have.

5 Q. When did you last see it? 10:50:16

6 A. Yesterday.

7 Q. Is it in your binder?

8 A. Yes, it is.

9 Q. Okay. So turning to Exhibit 4, what is
10 it? 10:50:31

11 A. This is an internal Google web page,
12 again, internal Google site page with some
13 information.

14 Q. Okay. This document is titled [REDACTED]
15 [REDACTED] 10:50:47

16 Do you see that?

17 A. I do.

18 Q. Do you have an understanding -- well, let
19 me ask this: What does that mean?

20 A. It details [REDACTED] 10:50:54
21 [REDACTED]

22 [REDACTED]

23 Q. And -- and would that include the sources
24 for the logs that we have been discussing today,
25 thus far? 10:51:13

CERTIFICATE OF REPORTER

I, Hanna Kim, a Certified Shorthand Reporter, do hereby certify:

That prior to being examined, the witness in the foregoing proceedings was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth;

That said proceedings were taken before me at the time and place therein set forth and were taken down by me in shorthand and thereafter transcribed into typewriting under my direction and supervision;

I further certify that I am neither counsel for, nor related to, any party to said proceedings, not in anywise interested in the outcome thereof.

Further, that if the foregoing pertains to the original transcript of a deposition in a federal case, before completion of the proceedings, review of the transcript [X] was [] was not requested.

In witness whereof, I have hereunto subscribed my name.

Dated: April 12, 2021



Hanna Kim, CLR, CSR No. 13083

EXHIBIT 143

6/11/21 David Monsees Deposition Transcript Excerpts

CONFIDENTIAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, ELAINE CRESPO,)
HADIYAH JACKSON and CLAUDIA)
KINDLER, on behalf of all)
others similarly situated,)
Plaintiffs,)
vs.) Case No.
GOOGLE LLC,) 5:20-cv-5146-LHK
Defendant.)
_____)

CONFIDENTIAL

VIRTUAL VIDEOCONFERENCE VIDEO-RECORDED
DEPOSITION OF DAVID MONSEES, VOLUME 2

Friday, June 11, 2021
Testifying from San Francisco, California

Reported By:
Hanna Kim, CLR, CSR No. 13083
Job No. 4624328

Page 359

CONFIDENTIAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

PATRICK CALHOUN, ELAINE CRESPO,)
HADIYAH JACKSON and CLAUDIA)
KINDLER, on behalf of all)
others similarly situated,)
Plaintiffs,)
vs.) Case No.
GOOGLE LLC,) 5:20-cv-5146-LHK
Defendant.)
_____)

Confidential, virtual videoconference
video-recorded deposition of DAVID
MONSEES, VOLUME 2, taken on behalf of the
Plaintiffs, testifying from San Francisco,
California, on Friday, June 11, 2021,
before Hanna Kim, CLR, CSR No. 13083.

CONFIDENTIAL

REMOTE VIDEOCONFERENCE APPEARANCES OF COUNSEL:

For Plaintiffs:

BLEICHMAR FONTI & AULD LLP

BY: LESLEY WEAVER, ESQ.

BY: ANGELICA M. ORNELAS, ESQ.

555 12th Street, Suite 1600

Oakland, California 994607

415.445.4003

lweaver@bfalaw.com

aornelas@bfalaw.com

-and-

KAPLAN FOX & KILSHEIMER LLP

BY: DAVID A. STRAITE, ESQ.

850 Third Avenue

New York, New York 10022

212.687.1980

dstraite@kaplanfox.com

Page 361

REMOTE VIDEOCONFERENCE APPEARANCES (CONTINUED)

For Plaintiffs:

SIMMONS HANLY CONROY LLC

BY: JASON "JAY" BARNES, ESQ.

112 Madison Avenue, 7th Floor

New York, New York 10016

212.784.6400

jaybarnes@simmonsfirm.com

For Defendant Google LLC:

QUINN EMANUEL URQUHART & SULLIVAN

BY: ANDREW H. SCHAPIRO, ESQ.

191 N. Wacker Drive, Suite 2700

Chicago, Illinois 60606

312.705.7400

andrewschapiro@quinnemanuel.com

-and-

BY: JOSEF ANSORGE, PH.D.

1300 I Street NW, Suite 900

Washington, D.C. 20005

202.538.8000

josefansorge@quinnemanuel.com

CONFIDENTIAL

1 response, receive response. So it --

2 Q. Right.

3 So to be clear from the -- your -- the

4 last time you said, well, you didn't know if it

5 was received. In this case, it was received; 11:28:01

6 correct?

7 A. Yeah, I think HTTP status codes are a -- a

8 pretty common thing. I won't say I'm an expert in

9 most, but I believe 200 is a successful

10 transmission and -- 11:28:14

11 Q. Okay.

12 A. -- and this says 200.

13 Q. And to the extent any screenshot would go

14 through today and does not have that, that's

15 merely a function of not having -- wanting to give 11:28:24

16 all of our eyes a break and get -- rather than

17 squeezing as much as possible on the screen. So

18 every time I ask you a question, there is a

19 response code that is "OK" in the native file.

20 Back to the DS -- to the IDE values at 11:28:40

21 DoubleClick.net, you agree that that value is

22 transferred to DoubleClick.net regardless of the

23 user's sync state?

24 A. Correct. Cookies for all domains have

25 nothing do with sync state or the browser type 11:29:01

Page 469

CONFIDENTIAL

1 that you're using. They're always transmitted
2 since Mosaic, I think, back -- back in the day.

3 Q. Okay. And regarding other data Google
4 receives from this transmission, Google would --
5 would receive the user's IP address; correct? 11:29:18

6 A. As with any other browser or any server,
7 that is correct.

8 Q. And specifically with regards to this, it
9 would receive the IP address regardless of the
10 Chrome user's current sync state; correct? 11:29:34

11 A. Correct. Total --

12 Q. And that's --

13 THE COURT REPORTER: I'm sorry. What was
14 the last part. "Total"?

15 THE WITNESS: Totally orthogonal or 11:29:46
16 independent of.

17 BY MR. BARNES:

18 Q. And that's true for all Chrome users;
19 correct?

20 A. Yes, that is correct. 11:29:53

21 Q. And Google would also receive the specific
22 user agent associated with this instance of
23 Chrome; correct?

24 A. And true with any browser, the browser
25 defines the user agent, which is sent in every 11:30:13

Page 470

CONFIDENTIAL

1 HTTP request.

2 Q. So I asked about -- I'm asking about the
3 Chrome browser, not every browser.

4 Google would receive for this HTTP request
5 the user agent of the Chrome browser in question; 11:30:28
6 correct?

7 A. Correct, which says Mozilla, AppleWebKit,
8 and Chrome and Safari here.

9 Q. And it would -- Google would receive that
10 data from the Chrome browser regardless of the 11:30:41
11 Chrome user's sync state; correct?

12 A. Correct. DoubleClick.net, the server that
13 that domain points to, would receive the request,
14 regardless of not just Sync, but Chrome or Firefox
15 or an application endpoint, anything. 11:30:58

16 Q. Okay. And Google also receives the
17 X-Client-Data information from this Chrome
18 browser; correct?

19 A. In this request, yes, I see it under
20 "Miscellaneous." 11:31:11

21 Q. Now, for X-Client-Data, Google would not
22 always receive that -- that number string;
23 correct?

24 A. I believe that Chrome clients, but I don't
25 know if all Chrome clients will send the 11:31:26

Page 471

CONFIDENTIAL

1 X-Client-Data value regardless of sync state for
2 the -- the anonymous experiment ID list.

3 Q. So the X-Client would not be transmitted
4 from Chrome to Google, if a user was in incognito
5 mode; correct? 11:31:53

6 A. That's correct. That's correct.

7 Q. And X-Client-Data would not be transmitted
8 to Google if -- for any browser other than Chrome;
9 correct?

10 A. That is correct. My understanding is a 11:32:01
11 Chrome unique header.

12 Q. Okay. And Google also receives this
13 "Referer" header information.

14 Do you see that?

15 A. I do. 11:32:15

16 Q. And what is the referer header in this
17 case?

18 A. The referer is a standard HTTP header. It
19 applies to all browsers, and it identifies the
20 page making the request and -- 11:32:29

21 Q. And --

22 THE COURT REPORTER: One sec. There's
23 some talking over. "Making the request"?

24 THE WITNESS: Apologies, Hanna.

25 To -- to continue that, in this case the 11:32:38

Page 472

CONFIDENTIAL

JURAT

I, DAVID MONSEES, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on the 11th day of June, 2021; that I have made such corrections as appear noted herein in ink, initialed by me; that my testimony as contained herein, as corrected, is true and correct.

Dated this _____ day of _____, 2021,
at _____.

DAVID MONSEES

EXHIBIT 144

3/17/22 Porter Felt 30(b)(6) Deposition Transcript Excerpts

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CHASOM BROWN, WILLIAM BYATT,)
JEREMY DAVIS, CHRISTOPHER) CASE NO.:
CASTILLO, AND MONIQUE TRUJILLO,) 5:20-cv-03664-
INDIVIDUALLY AND ON BEHALF OF) LHK-SVK
ALL OTHER SIMILARLY SITUATED,)
Plaintiffs,)
v.)
GOOGLE, LLC,)
Defendant.)

DEPOSITION OF DR. ADRIENNE PORTER FELT, VOL. I
TAKEN ON BEHALF OF THE PLAINTIFFS
REMOTELY VIA ZOOM VIDEO CONFERENCING, IN
MOUNTAIN VIEW, CALIFORNIA, BEGINNING AT
2:47 P.M. AND ENDING AT 6:52 P.M., ON
THURSDAY, MARCH 17, 2022, BEFORE
NATALIE PARVIZI-AZAD, CERTIFIED SHORTHAND
REPORTER NUMBER 14125.

A P P E A R A N C E S

FOR THE PLAINTIFF, CHASOM BROWN, WILLIAM BYATT,
JEREMY DAVIS, CHRISTOPHER CASTILLO, AND MONIQUE
TRUJILLO, INDIVIDUALLY AND ON BEHALF OF ALL OTHER
SIMILARLY SITUATED:

BOIES SCHILLER FLEXNER
BY: BEKO REBLITZ-RICHARDSON, ESQ.
BY: ERIKA NYBORG-BURCH, ESQ.
44 MONTGOMERY STREET
41ST FLOOR
SAN FRANCISCO, CALIFORNIA 94104
(415) 293-6800
BRICHARDSON@BSFLLP.COM
ENYBORG-BURCH@BSFLLP.COM

FOR THE PLAINTIFFS IN "CALHOUN V GOOGLE":
BLEICHMAR FONTI AND AULT
BY: ANGELICA M. ORNELAS, ESQ.
555 12TH STREET
SUITE 1600
OAKLAND, CALIFORNIA 94607
(415) 445-4011
AORNELAS@BFALAW.COM

APPEARANCES CONTINUED ON THE FOLLOWING PAGE.

A P P E A R A N C E S

FOR THE DEFENDANTS, GOOGLE, LLC:

QUINN EMANUEL URQUHART AND SULLIVAN

BY: JOMARIE CRAWFORD, ESQ.

51 MADISON AVENUE

22ND FLOOR

NEW YORK, NEW YORK 10010

(212) 849-7581

JOMAIRECRAWFORD@QUINNEMANUEL.COM

- AND -

QUINN EMANUEL URQUHART AND SULLIVAN

BY: ALY OLSON, ESQ.

65 S. FIGUEROA STREET

10TH FLOOR

LOS ANGELES, CALIFORNIA 90017

(213) 443-3000

ALYOLSON@QUINNEMANUEL.COM

ALSO PRESENT:

JOANN YAGER, VIDEOGRAPHER;

MATTHEW GUBIOTTI, IN-HOUSE COUNSEL AT GOOGLE

I N D E X

WITNESS	PAGE
DR. ADRIENNE PORTER FELT	
EXAMINATION BY MR. REBLITZ-RICHARDSON	8
EXAMINATION BY MS. CRAWFORD	100
EXAMINATION BY MR. REBLITZ-RICHARDSON	108

E X H I B I T S

EXHIBIT NO.	DESCRIPTION	PAGE
EXHIBIT 1	30(B)(6) DEPOSITION NOTICE	9
EXHIBIT 2	30(B)(6) DEPOSITION NOTICE	10
EXHIBIT 3	E-MAIL CHAIN LAST DATED DECEMBER 10, 2018; BATES GOOGCABR03827263	82
EXHIBIT 4	PRIVACY POLICY	82
EXHIBIT 5	CHROME SUBSCRIPTIONS OPPORTUNITY ASSESSMENT; BATES GOOGBRWN00163177	86
EXHIBIT 6	MARCH 31ST, 2020, VERSION OF GOOGLE'S PRIVACY POLICY	101

INSTRUCTIONS NOT TO ANSWER

PAGE	LINE
12	15
30	13

1 Incognito mode, Google Analytics might still be
2 included in the page. However -- actually,
3 that's it.

4 Q. And as a result, would Google receive
5 information regarding that user's private 03:31:59
6 browsing visit to Williams-Sonoma?

7 MS. CRAWFORD: Objection to the form of
8 the question.

9 THE WITNESS: What kind of information
10 are you talking about? 03:32:11

11 BY MR. REBLITZ-RICHARDSON:

12 Q. Any information.

13 MS. CRAWFORD: Vague and overbroad.

14 THE WITNESS: In order for Google to
15 fulfill the request, because of how internet 03:32:25
16 networking works, Google would see, for example,
17 the user's IP address in order to respond and
18 provide the script or other way that the service
19 has been embedded.

20 BY MR. REBLITZ-RICHARDSON: 03:32:40

21 Q. Other than the user IP address, would
22 Google receive any information when a user
23 visited Williams-Sonoma in a private browsing
24 mode such as Chrome Incognito?

25 MS. CRAWFORD: Objection to the form of 03:32:56

1 the question. It's an incomplete hypothetical.

2 THE WITNESS: I'm not sure I can -- can
3 you be more specific about what type of data
4 you're asking about?

5 BY MR. REBLITZ-RICHARDSON: 03:33:20

6 Q. Any data that Google received when
7 someone in a private browsing mode such as
8 Chrome Incognito goes to Williams-Sonoma?

9 A. So the browser would send the IP
10 address as part of fulfilling their request. 03:33:32
11 As part of the header -- or sorry. As -- part
12 of the request might specify, for example,
13 language of the device, and cookies might be
14 attached to the request using the clean cookie
15 jar that is used in Incognito mode. 03:34:00

16 Q. What about user agent?

17 A. Yes, the user agent string would
18 include basic information that is attached to
19 all web resource requests.

20 Q. What about location information? 03:34:23

21 A. What do you mean by location
22 information?

23 Q. Any geolocation information. Any
24 location tied to the user or the device.

25 MS. CRAWFORD: Same objection as 03:34:55

1 before. Vague. Incomplete hypothetical.

2 THE WITNESS: It would depend on the
3 implementation of Williams-Sonoma. And I'm also
4 not an expert on either Williams-Sonoma or
5 Google Analytics, like how they specifically 03:35:26
6 work, so I can't really answer that specific
7 example.

8 BY MR. REBLITZ-RICHARDSON:

9 Q. Any unique identifiers that Google
10 would collect when a user visits 03:35:31
11 Williams-Sonoma in a private browsing mode?

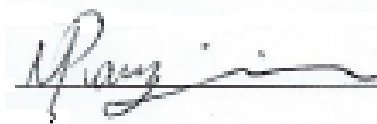
12 A. I'm going to step away from the
13 Williams-Sonoma example because I don't know
14 exactly how it works, but I can answer more
15 generally. 03:35:53

16 When you are using Incognito, you have
17 a fresh -- the user has a fresh cookie store,
18 meaning that by default, once you've opened up
19 the new incognito tab, you are not signed into
20 your Google account, and cookies from your 03:36:02
21 main, not Incognito session, are not carried
22 over. Now, if a user chooses to sign in to a
23 website after that point, you know,
24 (indiscernible), they then could be signed into
25 something in an Incognito window. I use 03:36:24

1 I HAVE NOT, AND SHALL NOT, OFFER OR PROVIDE
2 ANY SERVICES OR PRODUCTS TO ANY PARTY'S ATTORNEY
3 OR THIRD PARTY WHO IS FINANCING ALL OR PART OF THE
4 ACTION WITHOUT FIRST OFFERING SAME TO ALL PARTIES
5 OR THEIR ATTORNEYS ATTENDING THE PROCEEDING AND
6 MAKING SAME AVAILABLE AT THE SAME TIME TO ALL
7 PARTIES OR THEIR ATTORNEYS. (CIV. PROC §
8 2025.320(B))

9 I SHALL NOT PROVIDE ANY SERVICE OR PRODUCT
10 CONSISTING OF THE CERTIFIED STENOGRAPHER'S
11 NOTATIONS OR COMMENTS REGARDING THE DEMEANOR OF
12 ANY WITNESS, ATTORNEY, OR PARTY PRESENT AT THE
13 PROCEEDING TO ANY PARTY OR ANY PARTY'S ATTORNEY OR
14 THIRD PARTY WHO IS FINANCING ALL OR PART OF THE
15 ACTION, NOR SHALL I COLLECT ANY PERSONAL
16 IDENTIFYING INFORMATION ABOUT THE WITNESS AS A
17 SERVICE OR PRODUCT TO BE PROVIDED TO ANY PARTY OR
18 THIRD PARTY WHO IS FINANCING ALL OR PART OF THE
19 ACTION. (CIV. PROC. § 2025.320(C))

20 DATED: MARCH 22, 2022

21
22
23
24 

25 NATALIE PARVIZI-AZAD, CSR NO.14125

EXHIBIT 145

8/19/21 Brian Rakowski Deposition Transcript Excerpts

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

---oOo---

CHASOM BROWN; MARIA NGUYEN;
WILLIAM BYATT; JEREMY DAVIS;
and CHRISTOPHER CASTILLO,
individually and on behalf
of all other similarly
situated,

Plaintiffs,

vs.

No. 5:20-cv-03664-LHK

GOOGLE LLC,

Defendant.

_____/

CONFIDENTIAL

REMOTE VIDEOTAPED DEPOSITION OF BRIAN RAKOWSKI

THURSDAY, AUGUST 19, 2021

Stenographically Reported by:

ANDREA M. IGNACIO, CSR, RPR, CRR, CCRR, CLR

California CSR No. 9830

Job No. 741808

MAGNA LEGAL SERVICES

866-624-6221

www.MagnaLS.com

1 R E M O T E A P P E A R A N C E S :

2

3

4 COUNSEL FOR THE PLAINTIFFS:

5 BOIES SCHILLER & FLEXNER LLP

6 By: BEKO RICHARDSON, ESQ.

7 MARC C. MAO, ESQ.

8 ERIKA NYBORG-BURCH, ESQ.

9 44 Montgomery Street, 41st Floor

10 San Francisco, California 94104

11

12 BOIES SCHILLER & FLEXNER LLP

13 By: ROSSANA BAEZA, ESQ.

14 100 SE 2nd Street, 28th Floor

15 Miami, Florida 33131

16

17 MORGAN & MORGAN

18 By: RYAN MCGEE, ESQ.

19 RA AMEN, ESQ.

20 201 N. Franklin Street, 7th Floor

21 Tampa, Florida 33602

22

23

24

25

1 R O M O T E A P P E A R A N C E S : (Cont.)

2

3

4 COUNSEL FOR THE DEFENDANT:

5 QUINN EMANUEL URQUHART & SULLIVAN

6 By: VIOLA TREBICKA, ESQ.

7 TEUTA FANI, ESQ.

8 865 S. Figueroa Street, 10th Floor

9 23 Los Angeles, California 90017

10

11

12 ALSO PRESENT: Matthew Gubiotti, Google

13 Evan Tsilimidos, Videographer

14 Vanessa Wheeler, Exhibit Technician

15 ---oOo---

16

17

18

19

20

21

22

23

24

25

1 INDEX OF STATEMENT

2

3 WITNESS: Brian Rakowski

4

5 EXAMINATION PAGE

6 By Mr. Richardson 12, 320

7 By Mr. Trebicka 318

8

9 INDEX OF DEPOSITION EXHIBITS

10 EXHIBIT PAGE

11 Exhibit 2 6-10-08 E-mail, Re: Chrome 68

12 top 10 - mk, Bates

13 GOOG-BRWN-00228744.R - '745.R

14 Exhibit 3 6-12-08 E-mail, Re: Chrome 85

15 Closing Interviews Today -

16 Summary of P2, P6, P5, Bates

17 GOOG-BRWN-00228597 - '99

18 Exhibit 4 7-11-08 E-mail, Re: Chrome 103

19 redirect loop issue - observation

20 Bates GOOG-BRWN-00410076

21 Exhibit 5 7-11-08 E-mail, Chrome redirect 120

22 loop issue - observation

23 Bates GOOG-BRWN-00226894 - '95

24 Exhibit 6 7-17-18 E-mail, Chrome Team Meeting 135

25 Notes, Bates GOOG-BRWN-00409986 - '87

1 to stop with the speaking objections. You can make 09:30
2 your objections, but your coaching of the witness is 09:30
3 improper. 09:30

4 I'd ask that the court reporter please read 09:30
5 back the question. 09:30

6 (Whereupon, record read by the Reporter as 09:30
7 follows: 09:30

8 "Question: So when -- when someone is -- is 09:29
9 browsing using Google's Chrome Incognito 09:29
10 Mode, does Google ever collect or receive 09:29
11 any information regarding that person's 09:29
12 browsing history?") 09:29

13 THE WITNESS: In my understanding of your 09:30
14 question, no. 09:30

15 MR. RICHARDSON: Q. And -- and can you 09:30
16 explain that to me. 09:30

17 Why would Google never receive information 09:30
18 regarding that person's browsing history? 09:30

19 MS. TREBICKA: Objection; misstates 09:31
20 testimony; vague. 09:31

21 THE WITNESS: To me, I'd like to under- -- 09:31
22 I'm responding to the question about browsing history. 09:31
23 To me, that has a very -- a specific meaning, to which 09:31
24 I would say no. 09:31

25 MR. RICHARDSON: Okay. That's helpful. 09:31

1 Q What do you understand "browsing history" to 09:31
2 mean? 09:31

3 A Browsing history in the browser is a list of 09:31
4 websites that you have visited in the past. The 09:31
5 browser maintains this list to help people re-navigate 09:31
6 to pages they have been to. 09:31

7 Q Thank you. 09:31

8 When people are browsing using Google's 09:31
9 Chrome Incognito Mode, does Google ever collect or 09:31
10 receive the person's IP address? 09:32

11 MS. TREBICKA: Objection; vague and compound. 09:32

12 Go ahead. 09:32

13 THE WITNESS: Yes. If a user navigates to a 09:32
14 site that contains request URL, request to a Google 09:32
15 server, it must get the IP address. 09:32

16 MR. RICHARDSON: Q. When people are browsing 09:32
17 using Google's Chrome Incognito Mode, does Google ever 09:32
18 collect or receive the person's browser user agent? 09:32

19 MS. TREBICKA: Objection; vague and compound. 09:32

20 THE WITNESS: Yes. In the case where one of 09:32
21 the requests goes to a Google server, it must receive 09:32
22 the user agent in order to respond to the request. 09:32

23 MR. RICHARDSON: Q. When people are browsing 09:32
24 using Google's Chrome Incognito Mode, does Google ever 09:32
25 collect or receive information regarding that person's 09:32

1 physical location? 09:32

2 MS. TREBICKA: Objection; vague and compound. 09:33

3 THE WITNESS: Physical location, no. 09:33

4 MR. RICHARDSON: Thank you. 09:33

5 Q When people are browsing using Google's 09:33

6 Chrome Incognito Mode, does Google ever collect unique 09:33

7 identifiers tied to that person? 09:33

8 MS. TREBICKA: Objection; vague and compound. 09:33

9 THE WITNESS: I'd have to understand what you 09:33

10 mean by "unique identifier." It's a very general term 09:33

11 in the industry. 09:33

12 MR. RICHARDSON: Let me change the question. 09:33

13 Q When people are browsing using Google's 09:33

14 Chrome Incognito Mode, does Google ever collect any 09:33

15 identifiers? 09:33

16 MS. TREBICKA: Objection; vague and compound. 09:33

17 THE WITNESS: "Identifier" is a -- again, a 09:34

18 tricky one, but let me -- let me try my best. 09:34

19 If you make a request to a Google server in 09:34

20 any browsing mode, including Incognito, a new cookie 09:34

21 will be set. That is part of the way the -- the web 09:34

22 works. And that cookie can -- you could -- could 09:34

23 contain identifiers, depending on what the server -- 09:34

24 you know, how it's configured. 09:34

25 MR. RICHARDSON: Got it. 09:34

1 MR. RICHARDSON: Yes. 09:54

2 THE WITNESS: Obviously, there's lots of 09:54

3 other -- other ways it's used. 09:54

4 In -- in Internet technology, there's a 09:54

5 technique that some websites use where you would 09:54

6 combine all kinds of information about a request to 09:54

7 try to identify who -- to try to -- to identify a user 09:54

8 or a group of users. 09:54

9 MR. RICHARDSON: Q. And what types of 09:54

10 information might a website use to try and identify a 09:54

11 user or group of users? 09:54

12 MS. TREBICKA: Objection; calls for 09:54

13 speculation. 09:54

14 THE WITNESS: In -- in my understanding of -- 09:54

15 of the -- the technique at the -- you would use a 09:55

16 combination of the -- the cookie -- any cookies you 09:55

17 might have, other information about which extensions 09:55

18 or plug-ins might be installed, the version number of 09:55

19 the -- of the user agent requesting information, and 09:55

20 combine that information to -- to get a -- to -- to 09:55

21 get a -- a fingerprint, so to speak. 09:55

22 MR. RICHARDSON: Q. You mentioned in your 09:55

23 answer cookies, information about extension/plug-ins, 09:55

24 version number of user agent. Those are the three 09:55

25 pieces of information you identified. 09:56

1 Is there any other information that you're 09:56
2 aware of that can be used for fingerprinting? 09:56

3 A Let me -- let me think. This is -- I haven't 09:56
4 thought about this in a long time. 09:56

5 There -- there -- there almost certainly is, 09:56
6 you know, even very mundane information the -- the 09:56
7 technique attempts to include. I don't know off the 09:56
8 top of my head what else might be included. But 09:56
9 almost certainly, there's more -- more information 09:56
10 that you would try to use. 09:56

11 Q What are the mundane types of information 09:56
12 that might be used in fingerprinting? 09:56

13 A Any other information that might be conveyed 09:56
14 in a -- in a header that would be sent. Yeah, I can 09:56
15 vaguely remember some -- some somewhat esoteric 09:57
16 fingerprinting case studies or white papers or reports 09:57
17 that I had heard where some information would be -- 09:57
18 would be most accidentally sent as part of a bug in 09:57
19 the way the web platform worked, but I can't remember 09:57
20 what those -- what those things were. 09:57

21 Q You referred to information in a header. 09:57

22 What's a header? 09:57

23 A A header is the first part of an HTTP 09:57
24 request, which includes information like the protocol 09:57
25 that is being used, the user agent, the IP address. 09:57

1 There -- there are -- there can be many different -- 09:57

2 it's very extensible. So different browsers can send 09:58

3 many, many different headers. 09:58

4 MS. TREBICKA: We've been going for about an 09:58

5 hour. Whenever is a good time in -- in your flow, 09:58

6 Beko, I'd like to ask for a break, unless Mr. Rakowski 09:58

7 needs a break sooner. But I just wanted to lodge that 09:58

8 request. 09:58

9 MR. RICHARDSON: If it's okay with you, 09:58

10 Mr. Rakowski, we'll just go about ten more minutes, 09:58

11 and then take a break. 09:58

12 THE WITNESS: Works for me. 09:58

13 MS. TREBICKA: Okay. Thank you, Beko. 09:58

14 MR. RICHARDSON: Q. You mentioned IP 09:58

15 address. 09:58

16 Is IP address part of the kind of category of 09:58

17 information that can be used for fingerprinting? 09:58

18 A Yes. Anything that comes with the request 09:58

19 would be -- could be used. 09:58

20 Q When you say anything that comes with the 09:58

21 H -- the request, you mean anything that comes with 09:58

22 the HTTP request; is that right? 09:58

23 A Exactly, yes. 09:58

24 Q And when someone is using the Chrome 09:59

25 Incognito Mode, does Google receive any of the 09:59

1 information from the HTTP -- HTTP request? 09:59

2 MS. TREBICKA: Objection; vague and compound. 09:59

3 THE WITNESS: Yes. The -- the HTTP request 09:59

4 is -- is made as part of a browsing session in 09:59

5 Incognito. 09:59

6 MR. RICHARDSON: Q. And on what occasions 09:59

7 would that information be collected by Google? 09:59

8 A If you -- if you'd restate to -- to "received 09:59

9 by Google." "Collected" seems -- could mean lots of 09:59

10 things. 09:59

11 But received -- it would be received in any 09:59

12 situation where a request in the page came to a Google 09:59

13 server. 09:59

14 Q And what are the sorts of occasions where a 10:00

15 request could come to a Google server? 10:00

16 Would that include, for example, when there 10:00

17 is a Google Analytics or Google Ad Manager script on 10:00

18 the website? 10:00

19 MS. TREBICKA: Objection; compound. 10:00

20 THE WITNESS: The types of situations is when 10:00

21 a user requests a page on google.com, for instance, or 10:00

22 when the page they request embeds content from Google. 10:00

23 MR. RICHARDSON: Q. And what are some of the 10:00

24 examples of when a web page would embed content from 10:00

25 Google? 10:00

1 requests, and then take the response back. 10:47

2 MR. RICHARDSON: Q. Have you read the 10:47

3 complaint filed in this lawsuit? 10:47

4 A Yesterday. I didn't read the whole thing. 10:47

5 I -- I -- I did page through it. 10:47

6 Q And are you generally familiar with the 10:47

7 allegations in this lawsuit? 10:47

8 A Generally familiar, yeah. 10:47

9 Q And do you understand that this lawsuit 10:47

10 concerns, in part, Google's collection, storage, and 10:47

11 use of private browsing information? 10:47

12 A Yes. I saw that in the document. 10:48

13 Q And you understand that that -- the focus is 10:48

14 on Google as the entity that's collecting, storing, 10:48

15 and using private browsing information; correct? 10:48

16 A Yes. 10:48

17 Q And so what I'm trying to understand here is, 10:48

18 you're talking about sending, receiving, processing, 10:48

19 recording, and collecting as different categories. 10:48

20 And I want to focus on those with respect to Google. 10:48

21 So when someone visits a third-party website 10:48

22 that uses Google services, like Google Analytics and 10:48

23 Google Ad Manager, how is it that information from 10:48

24 that private browsing is sent to Google? 10:48

25 A So -- 10:48

1 MS. TREBICKA: Objection; vague. Objection; 10:48

2 vague, and also -- and also to the extent that it 10:48

3 calls for speculation. 10:48

4 Go ahead. 10:48

5 THE WITNESS: Yeah, I was -- sorry for 10:48

6 talking over you. 10:48

7 The -- I don't know how all those web 10:48

8 services work. I'm the -- I'm knowledgeable about how 10:49

9 the browser was designed and implemented, but I don't 10:49

10 know the -- the back end side of the -- those 10:49

11 services. 10:49

12 MR. RICHARDSON: Okay. 10:49

13 Q But if those Google services are receiving, 10:49

14 for example, the IP address or the user agent, that's 10:49

15 information that they're receiving from the Chrome 10:49

16 browser; is that correct? 10:49

17 MS. TREBICKA: Objection; vague and calls for 10:49

18 speculation. 10:49

19 Go ahead. 10:49

20 THE WITNESS: Yeah, in the context of what we 10:49

21 just talked about, when you submit -- when you issue a 10:49

22 request from the browser, so as the user -- on behalf 10:49

23 of the user, the user agent issues a request to a 10:49

24 server. That request contains the -- all the standard 10:49

25 browser header information, including IP address, 10:49

1 user-agent string, those -- those parts of the -- the 10:49

2 protocol. 10:49

3 MR. RICHARDSON: Q. And that is the browser 10:49

4 header information that is sent to and received by 10:50

5 Google when there is a use of Google services; 10:50

6 correct? 10:50

7 A Correct, when there is a use of Google 10:50

8 services. 10:50

9 Q Okay. Going back to Exhibit 2, does this at 10:50

10 least indicate to you that the name Incognito was 10:50

11 selected sometime prior to June 2008? 10:50

12 A Yeah, as -- well, as of two -- as of this 10:50

13 date, it seems like that's the name that Michael 10:50

14 thinks we would -- we would go with. 10:50

15 I'm just looking through the rest of the doc 10:50

16 real quick. There aren't actually many other names. 10:50

17 So I don't know how far along we were in the process 10:50

18 of finalizing our -- our names. 10:50

19 But at least he's -- he's -- his e-mail 10:50

20 presumes that that is the feature name. 10:50

21 Q And going back to, you know, choose Incognito 10:51

22 Mode for private browsing, you -- you stated that 10:51

23 private browsing could mean different things; is that 10:51

24 right? 10:51

25 MS. TREBICKA: Objection to the extent -- 10:51

1 THE WITNESS: Yes. 10:51

2 MS. TREBICKA: -- it misstates prior 10:51

3 testimony. 10:51

4 Go ahead. 10:51

5 MR. RICHARDSON: Q. Do you believe that it 10:51

6 is accurate to describe Incognito Mode as private 10:51

7 browsing? 10:51

8 A Context is important for that one. In -- in 10:51

9 the context of what other browsers have done, I 10:51

10 believe their implementation is similar to ours, 10:51

11 although I'm not -- I haven't studied them. So from 10:51

12 that perspective, it might -- it might be analogous to 10:51

13 the -- to use the term. In other characterizations, I 10:51

14 wouldn't -- I don't know if I would use that 10:52

15 description. 10:52

16 Q Do you yourself describe Incognito Mode as a 10:52

17 private browsing mode? 10:52

18 A When -- sorry. Today, when asked by friends 10:52

19 about -- about it? 10:52

20 Or what do you mean? 10:52

21 Q Sure. Let's -- let's start there. 10:52

22 A No. I think -- I think I use -- I actually 10:52

23 probably use a fairly pedantic description, like, you 10:52

24 get a fresh cookie jar, and it's a fresh instance of 10:52

25 your browser. Maybe I'm too close to it, but that's 10:52

1 CERTIFICATE OF REPORTER

2

3 I, ANDREA M. IGNACIO, hereby certify that the
4 witness in the foregoing remote deposition was by me
5 remotely sworn to tell the truth, the whole truth, and
6 nothing but the truth in the within-entitled cause;

7 That said deposition was taken in shorthand
8 by me, a disinterested person, at the time and place
9 therein stated, and that the testimony of the said
10 witness was thereafter reduced to typewriting, by
11 computer, under my direction and supervision;

12 That before completion of the deposition,
13 review of the transcript [x] was [] was not
14 requested. If requested, any changes made by the
15 deponent (and provided to the reporter) during the
16 period allowed are appended hereto.

17 I further certify that I am not of counsel or
18 attorney for either or any of the parties to the said
19 deposition, nor in any way interested in the event of
20 this cause, and that I am not related to any of the
21 parties thereto.

22 Dated:

23

24 _____
25 ANDREA M. IGNACIO, RPR, CRR, CCRR, CLR, CSR No. 9830